# City of Sherwood Police Department

## Small Unmanned Aircraft Systems

## Standard Operating Procedure (SOP) Manual

# Table of Contents

## 1. Purpose

The following procedures are intended to promote safe, efficient, and lawful operation of all Small Unmanned Aerial Systems (sUAS) operated by the City of Sherwood (COS) Police Department (SPD). Regardless of the nature of the mission, safety is the primary concern of every operation.

## 2. Philosophy

The operation of sUAS has the potential to influence the resources available to city staff, informing actions and increasing efficiencies in many departments. This far-reaching technology may be used to protect the lives and property of citizens and first responders, improve situational awareness during emergency response, and enhance services provided to the community.

It is the responsibility of every participating COS employee to contribute to the goal of ongoing safe sUAS operations. This contribution may come in many forms and includes always operating in a legal and safe manner while avoiding unnecessary risks. All participants engaged in the operation of sUAS have a responsibility to identify and mitigate potential safety hazards related to procedures, operations, or maintenance before an incident might occur.

SPD is committed to providing the best services possible to our community by ensuring our sUAS will be operated in a constitutionally and legally sound manner that respects and protects people's privacy and civil liberties. This means avoiding unneeded or unintended operation of sUAS without thoughtful consideration for personal privacy and public perception.

## 3. Administration

The policies and procedures contained in this document are issued under the authority of the Chief of Police. This sUAS Standard Operating Procedures Manual ("manual") is not intended to be all-inclusive, but rather to act as a supplement to department sUAS policy 605, FAA regulations and other documents, such as the user's manual provided by the manufacturer of the sUAS. This manual has been written to address sUAS rules and regulations as they existed when the document was drafted. Because an sUAS may be considered emerging technology, equipment, software, personnel, environmental conditions, regulations, etc., may change over time. Adaptive change management within the sUAS program involves a systematic approach to monitoring [SPD] organizational change and is a critical part of the risk management process for the operation of sUAS.

## 4. Protection of Rights and Privacy

Refer to Sherwood Police Department policy 605 - Unmanned Aerial Systems (sUAS) Operations for a statement on privacy.

SPD has specific requirements for the handling of sensitive information and protecting privacy in accordance with existing state and federal laws, but none shall conflict with the minimum requirements contained herein. SPD procedures for handling sensitive information are attached as Appendix A. Refer to applicable department policies on sUAS for more information.

**5. Definitions:**

**Small Unmanned Aircraft System (sUAS)**: An unmanned aircraft of any type (weighing less than 55 pounds) that is capable of sustaining directed flight, whether pre-programmed or remotely controlled and all of the supporting or attached systems designed for gathering information through imaging, recording or any other means. For the purpose of this SOP, an sUAS includes an "Unmanned Aircraft System (sUAS)," commonly referred to as a "drone", as defined by ORS 837.300

**14 CFR Part 107 (Part 107)**: Federal Aviation Administration (FAA) regulations regarding Small Unmanned Aircraft Systems. The certificate for 14 CFR Part 107 is also called a "remote pilot certificate".

**Aircrew Member**: Department personnel designated and selected as either (Pilot in Command) "PIC;" a "Student Operator;" or any personnel operating, observing as a crewmember or maintaining an sUAS.

**Certificate of Waiver**: A certificate issued by the Federal Aviation Administration authorizing a deviation from any regulation specified in 14 CFR §107.205

**Centralized Location**: With respect to training, operations, flight hours, maintenance, and other logs as noted in this SOP, centralized location refers to an online repository of program information. The current centralized location for the SPD sUAS Program is DroneSense.

**FAR**: Federal Aviation Regulations are rules published by the FAA that govern the use of any airspace above the ground within the United States of America.

**Hazard**: Something that has the potential to cause harm.

**Occurrence**: An unplanned safety related incident, including accidents or damage to aircraft or property.

**Pilot in Command (PIC)**: Is an sUAS operator who is certified under CFR 14 Part 107, approved by the program manager, and who has met specified requirements of knowledge, training, and operational proficiency. The PIC is directly responsible for the safety and operation of the sUAS. The PIC is the sole person responsible for control of the sUAS and has the final responsibility and authority to conduct flight operations within the National Airspace System as defined by the FAA. A student operator may operate under the direct supervision of a PIC for training purposes as approved by the program manager.

**Tactical Flight Officer (TFO)**: This person operates the camera payload, communicates and coordinates with ground resources and broadcasts radio communications. If there is not the capability to separately operate the camera payload, the TFO can be one who is watching the drone's camera feed and performing the same functions, without independently operating the camera.

**Program Coordinator**: The program coordinator is responsible for the overall direction and performance of the department sUAS program as defined by individual department policy. Refer to Section 6.1 for basic responsibilities of the program coordinator. A program coordinator will be assigned at the rank of sergeant and above.

**Student Operator**: An individual who has not yet earned a remote pilot certificate but is authorized to operate an sUAS by the program coordinator under the direct supervision of a PIC.

**Visual Observer (VO)**: An individual who assists the PIC and/or the person manipulating the controls of the sUAS to see and avoid other air traffic or objects aloft or on the ground. The use of a VO provides an optional and additional means of airspace and obstacle deconfliction. The use of a VO is mandatory for night flight operations.

**Mission:** A mission is defined as a flight that is not a training flight and has an official law enforcement purpose. An example of a mission is a flight conducted in search of a missing person, a block search for a suspect, or an overwatch flight to assist TNT with the service of a search warrant. A mission is also a flight for the collection of evidence in a crime scene or crash reconstruction.

## 6. Organization

The organizational structure for the operation of the sUAS includes SPD personnel functioning in the roles of program coordinator, PIC, TFOs, VOs, and student operators.

### 6.1 Program Coordinator

The program coordinator is responsible for the overall direction and performance of the department sUAS program. The responsibilities of the program coordinator for each department include but are not limited to:

- Report sUAS usage to the required governmental agencies on a yearly basis.
- Maintain and review program objectives, aircrew member training hours, performance and proficiency with sUAS.
- Approve and remove aircrew members from flight status as needed. Any aircrew member may be temporarily removed from flight status at any time by the program manager for reasons including, but not limited to, performance or proficiency.
- Liaison with the FAA as needed.
- Reviewing and updating program policies and procedures as needed.
- Evaluating each sUAS based on use and replacement needs.
- Monitoring the sUAS community to ensure best practices are incorporated into the SPD's use and operation of sUAS.

### 6.2 Pilot in Command (PIC)

The primary operational responsibility of the PIC is the safe and effective use of sUAS in accordance with the user's manual provided by the manufacturer, federal and state laws, and City policies and regulations. Ultimately, it is the responsibility of the PIC to ensure they meet current FAA and department qualifications to operate an sUAS.

### 6.3 Tactical Flight Officer (TFO)

The primary operational responsibilities of the TFO are the operation of the payload (camera) of the sUAS, the coordination of patrol units, and communication with those units and dispatch. The TFO is an active member of the aircrew and will typically possess a Part 107 remote pilot certificate. The TFO can transition to the PIC of an additional flight to take over a point of observation from the PIC on an active flight, which is referred to as a "Leapfrog." The TFO will be responsible for:

- Relaying pertinent information about what the aircrew is observing with the sUAS to the units responding to the call.
- All aircrew radio traffic to dispatch.
- Communicating with the PIC to gain the best possible point of observation over the call.
- Making sure the aircrew is video or screen recording (or sometimes both) the incident for documentation purposes.

**6.4 Visual Observers (VO)**
The role of a VO is to alert the PIC and the rest of the aircrew about potential hazards during sUAS operations. The use of a VO is only required during night operations. Although not required, a VO is recommended to enhance situational awareness during daylight operations when practical. The PIC may use one or more VOs to supplement situational awareness and visual loss of sight responsibilities. If a visual observer is used during the sUAS operation, all the following requirements must be met:

- The PIC (manipulating the flight controls of the sUAS) and the VO must maintain effective communication with each other at all times.
- The PIC must ensure the VO is able to see the sUAS and the position of other aircraft in the manner specified in 14 CFR §107.31.
- The PIC and the VO must coordinate to do the following:
    - Scan the airspace where the sUAS is operating for any potential collision hazard; and
    - Maintain awareness of the position of the sUAS through direct visual observation.

In addition to the requirements specified above, and only in coordination with the PIC, a VO may be asked to remain alert for suspicious persons or activities on the ground and coordinate a response through the PIC and incident command.

**6.5 Student Operators**
A student operator may operate an sUAS under the direct supervision of a PIC for training purposes as approved by the program coordinator. A student operator must be accompanied by a PIC at all times while at the controls of an sUAS. A student operator is responsible for the safety and operation of the sUAS, however, the PIC has final authority to direct a student operator of the sUAS at all times. Student operators may not operate an sUAS without PIC supervision until:

- All training requirements referenced in Section 8 of SOPs have been met.
- They possess a Part 107 remote pilot certificate.
- They are approved as a PIC by the program coordinator.

**7. Equipment Storage and Maintenance**
The SPD sUAS Team shall store and maintain equipment in a location and manner approved by the program coordinator and in compliance with manufacturer guidelines. In addition, all participating personnel are equally responsible for maintaining the equipment and facility in a neat, clean and orderly fashion. The sUAS shall be stored in a manner intended to prevent or reduce the probability of damage, tampering, or operation by unauthorized individuals. If batteries or controllers were used by a team member, that member will ensure the batteries and/or controller are placed onto the specified charger at the end of their shift. Team members utilizing an sUAS will return all equipment to the SPD storage location. sUAS equipment, to include batteries, will not be left in a vehicle at the end of their shift negatively affecting the integrity of the equipment.

**8. Training and Proficiency**

Before an aircrew member can function as a PIC, they must complete the following steps to demonstrate their knowledge of operational requirements and proficiency with individual sUAS aircraft:

- Complete at least twenty-four (24) hours of training in FAA rules and regulations, to include practice tests, through an approved training course at SPD expense.
- Pass the FAA Part 107 test and provide proof of certification to the Program Coordinator or designee. The department will pay for the initial FAA Part 107 test and coordinate the written exam. Further attempts to pass the exam will require consultation with the Program Coordinator to determine team member status.
- Have at least 40 hours of basic training encompassing basic flight skills, flight principles, and aviation safety. Understand legal regulations regarding sUAS use. Demonstrate best practices either through field deployments or organized training evaluated by the Program Coordinator or designee. Approve scenario-based training to include practical deployments.
- Show proficiency by passing the NIST course (Level 1) with a certified instructor.
- Receive final check-off by Program Supervisor through approved program checklist for each sUAS as a solo PIC.

The program coordinator has the authority to accept the SPD minimum training requirements of a PIC candidate based on the demonstrated proficiency and supportive training documentation of knowledge and experience. Lateral officers or team members already possessing a remote pilot certificate are eligible for this exemption.

For ongoing training, all flights or exercises will be documented and count toward an aircrew member's training. Aircrew members shall have a minimum of ten (10) hours of ongoing training per calendar year. This training should include, but is not limited to the following topics:

- Department commitment to safety
- Member's role in safety
- Review of sUAS program
- Emergency safety procedures
- Scenario-based training
- Medical conditions affecting operations and self-assessment
- Airspace
- FAA regulations
- Deployment
- Maintenance, repair, and storage of airframes
- sUAS performance
- Weather

All PICs shall maintain operational proficiency of sUAS. Aircrew members without any documented flight time within a span of 180 days will demonstrate operational proficiency with PIC checklist before functioning as PIC on a real-world event. Aircrew members may demonstrate operational proficiency on a real-world response or exercise in the role of a student operator at the discretion of, and under the direct supervision of, a current PIC. The program coordinator shall determine the amount required training (flight time and/or instructive) to demonstrate operational proficiency. All training shall be documented in the aircrew member’s file, maintained by the program coordinator or in a centralized system. It is incumbent on the aircrew member to ensure compliance and proper documentation of training and flight time. Failure to maintain or document operational proficiency can result in removal from sUAS responsibilities.

**9. Authorized Uses of sUAS**
See department sUAS policy 605 for authorized uses by department.

**10. Exigency**
The sUAS Team will continually weigh the exigency of a deployment against the requirement to obtain a search warrant when feasible. The PIC is responsible for the continual assessment of the mission and if it remains exigent, or if a warrant is required.
If the exigency of a mission appears to be diminishing, the PIC will assess whether to land the aircraft or to keep the point of observation while designating a warrant writer to begin the search warrant application process (based upon the circumstances of the case).

**11. Flight Checklists, Logs, and Registration**
Within the aviation community, the utilization of checklists and consistent sUAS documentation has significantly reduced the risk of aviation operations. As such, department PICs are required to utilize “DroneSense” to complete and maintain the logs and checklists listed in the proceeding subsections.

**11.1 Maintenance and Flight Logs**
- Maintenance of the equipment will be handled by the designated program member.
- The program coordinator, or designee, shall follow the maintenance schedule in the user’s manual provided by the manufacturer of the sUAS and maintain flight software/firmware as required.
- A maintenance log shall be established for each sUAS to track maintenance needs and repairs. The maintenance logs should be reviewed by the PIC before subsequent flights and updated after the last flight.
- If a mission is conducted, PICs shall complete a sUAS Team Daily Activity Report (DAR) documenting the time, location, duration, purpose of flight, and type of drone.
- PICs shall update the sUAS Team training flight log for all non-mission, training flight operations while on-duty.
- All maintenance records should be kept in the approved centralized location.

**11.2 Pre and Post Flight Checklists**
PICs are responsible for a thorough preflight inspection of the sUAS. Before and after each mission or training flight, the PIC shall:
- Conduct a thorough inspection of the sUAS in accordance with the user’s manual provided by the manufacturer. If the manufacturer does not provide a preflight checklist, the PIC must adopt and use the checklist provided as Appendix B to this manual.
- Check for physical equipment or firmware/software discrepancies. Any physical equipment or firmware/software discrepancy that cannot be resolved and which has a potential impact on flight safety will override the deployment of sUAS, and any discrepancy shall be resolved before flight. If issues are unresolved the sUAS will be removed from operation until all discrepancies have been resolved.
- Conduct a post flight inspection of the sUAS and document any discrepancies in the sUAS maintenance and appropriate flight log.

### 11.3 Registration
All sUAS used for SPD purposes shall be registered with the FAA and Oregon Department of Aviation. All SPD owned sUAS must also be recorded with Risk Management for insurance purposes. The program coordinator is responsible for ensuring all aircraft operated by the sUAS Team is properly registered with the Oregon Department of Aviation and the FAA. No personally owned sUAS equipment of any kind is authorized for official SPD use. SPD does not assume liability of any unauthorized sUAS equipment.

## 12. Record Keeping and Reporting
The program coordinator has the responsibility for maintaining team records. Aircrew member files shall be reviewed annually and should contain:

- Copies of FAA certifications and expiration dates
- Training records
- Flight logs for aircrew members
- Flight and maintenance records for each sUAS.

The program coordinator will ensure flight logs for each PIC are compiled and maintained in a centralized location. A combined summary of City of Sherwood Police Department flight logs will be submitted to the Oregon Department of Aviation by the program coordinator on a yearly basis.

## 13. sUAS Identification
All SPD's sUAS will be labeled or marked in the following ways:

- FAA and state registration numbers will be adhered to the sUAS as required by state and federal law.
- sUAS will display obvious visible features identifying it as City of Sherwood property, and these markings may appear as a colored label, sticker or covering (skin) on the sUAS.
- The color coding should have a high contrast value between the markings and the production color of the sUAS.
- A contact phone number will be displayed on the hull of the sUAS.

## 14. Deployment Priorities/Response Procedures
All sUAS operations within controlled airspace shall be conducted in accordance with Part 107 or an approved Certificate of Waiver. Command protocol, as defined in SPD Policy 200.3.1, has mission approval authority for operations but the PIC retains the final responsibility for the operation and safety of the sUAS. If requests for sUAS support are received simultaneously, they shall be prioritized with life safety as the highest priority. Field supervisors, command staff and officers will yield to the PIC's decision if the PIC decides the flight is either not safe or cannot be conducted according to the rules and regulations outlined in this manual, SPD Policy 605, the State of Oregon, or the FAA.

### 14.1 Deconfliction Procedures – Simultaneous Deployments
When two or more sUAS are assigned to the same incident, all sUAS shall maintain a safe vertical and horizontal distance as coordinated by the aircrew on the incident. During outdoor operations, that buffer shall be no less than 50 feet, if the PICs of both aircraft are launching from the same elevation. All aircrew operating in the same incident shall monitor and maintain voice communication over a common frequency when possible or in person. Deconfliction is the responsibility of each PIC. The incident commander should consider the risk versus benefit prior to authorizing a multi-sUAS operation. The primary agency on an incident has authority over air operations for that incident.

### 14.2 Crewed/Unmanned Aircraft Teaming

City of Sherwood Police Department sUAS operations may only be conducted in the vicinity of crewed aircraft when authorized by the FAA. Crewed aircraft always have the right of way and must always be avoided. In the event that Life Flight, wildland firefighting aircraft, or other rescue aircraft are activated for use on an incident, sUAS flight operations in the area of the incident must be terminated immediately upon notification of their activation unless operation of sUAS is requested by the incident commander and meets FAA requirements. When sUAS missions are conducted with crewed law enforcement aircraft, the PIC of the sUAS and the crewed aircrew should be communicated on the same radio frequency for proper altitude deconfliction.

## 15. Emergency Procedures

Emergency procedures are specific to each sUAS type as designed by the manufacturer. It is the responsibility of the flight crew to be proficient with the sUAS operational manual provided by the manufacturer before any flight operations are conducted. Many sUAS have a number of failsafe options in the event of signal loss. These options include the setting of a Home Location, Return to Home height setting, Automated Hover, or Return to Home mode. The specific failsafe options available for each type of sUAS should be outlined in the documentation for that sUAS (operator's manual, checklists, etc.).

### 15.1 Return Home Settings

- Return Home location must be selected, programmed and verified on the system map prior to every launch.
- Return Home location shall be an open area, clear of all obstructions.
- Appropriate Return Home altitude must be selected & programmed to avoid the tallest obstacle between operating the area and Return Home location.

### 15.2 Lost Link

- If signal link is lost for less than 5 seconds, the PIC will activate Return Home on the controller and verify that the signal link can be regained prior to subsequent flight.
- If signal link is lost with the sUAS for more than 5 seconds, the following procedures will be followed:
    - a. Immediate notification to Air Traffic Control, if required. Provide last known location, altitude, direction of travel, expected behavior/flight path.
    - b. Immediately notify the incident commander or supervisor. Give last known location, direction of travel, expected behavior/flight path.
    - c. Verify Return Home location is clear of obstructions.
    - d. Attempt to regain signal (troubleshoot remote control antenna position, operator position, line of sight, battery, device, cable and app)
    - e. If signal is not regained, visually verify automated return of sUAS or initiate sUAS recovery/mishap procedure.
    - f. If signal is regained, notify Air Traffic Control if required and the incident commander, and initiate a precautionary landing to verify condition of sUAS system components.

### 15.3 sUAS Recovery/Mishap Procedure

- The PIC will immediately notify the incident commander or supervisor and provide estimated location of the downed sUAS.
- Notify Air Traffic Control (if applicable).
- The incident commander will assign sUAS recovery resources.
- The sUAS will be treated as evidence and not tampered with except for the extent to safely recover the sUAS. The sUAS will be impounded and Risk management notified with the proper forms completed.
- The program coordinator will assign an investigator with the technical knowledge to determine the cause of the crash. The investigation, at a minimum, will document the required information list under “Accident Reporting” in Part 107. The findings will be forwarded up the chain of command within seven (7) days of the crash.
- The sUAS will not be returned to service until the program coordinator has determined the operational proficiency of the PIC and the airworthiness of the sUAS.

## 16. Occurrence and Hazard Reporting

The program coordinator shall establish or identify a hazard and/or occurrence reporting system. All reported hazards and/or occurrences will be investigated pursuant to established department policies. All flight crew members are authorized to take action to correct a hazard if in that member's opinion, delay will result in accident or injury. Findings of the program coordinator during the investigation of a hazard report shall be disseminated to the sUAS Team should the information be deemed worthy of reporting.

## 17. Complaints and Media Inquiries

sUAS Team members will follow SPD’s established policies and procedures regarding complaints and media inquiries.

## 18. Storage of Media and Data

sUAS Team members will follow SPD’s established policies and procedures, in compliance with all legal requirements. The sUAS Team is guided by the included policy on data retention and storage, labeled Appendix A.

# Appendix A

**Handling of Sensitive Information**

Policy **806**

City of Sherwood Police Department

Sherwood PD OR Policy Manual

# Protected Information

## 806.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the City of Sherwood Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Agency and not the public records information covered in the Records Maintenance and Release Policy.

806.1.1 DEFINITIONS

Definitions related to this policy include:

**Protected information** - Any information or data that is collected, stored or accessed by members of the City of Sherwood Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

## 806.2 POLICY

Members of the City of Sherwood Police Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

## 806.3 RESPONSIBILITIES

The Police Chief shall select a member of the Agency to coordinate the use of protected information.

The responsibilities of this position include but are not limited to:

(a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicle (DMV) records, and Law Enforcement Data System (LEDS).

(b) Developing, disseminating, and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy.

(c) Developing, disseminating, and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release, and security of protected information.

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

## 806.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, City of Sherwood Police Department policy or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution.

### 806.4.1 ACCESS TO OREGON STATE POLICE OFFENDER INFORMATION

Access to Oregon State Police (OSP) criminal offender information may be granted when the information is to be used for the administration of criminal justice, employment, or the information is required to implement a federal or state statute, local ordinance, Executive Order, or administrative rule that expressly refers to criminal conduct and contains requirements or exclusions expressly based on such conduct, or other demonstrated and legitimate needs (OAR 257-010-0025).

## 806.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Support Captain for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Agency may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Section to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other department members or the public is at risk. In those instances, cell phones should be used if possible.

The transmission should be limited to essential details only, with maximized use of law enforcement codes (10 or 12 code), concealing information identifying individuals and offenses as much as possible. Plain text transmission of an entire record (summary or full) is prohibited.

Nothing in this policy is intended to prohibit broadcasting warrant information.

### 806.5.1 REVIEW OF CRIMINAL OFFENDER RECORD

Individuals requesting to review their own Oregon criminal offender information shall be referred to OSP, Identification Services Section (OAR 257-010-0035).

An individual may review his/her local record on file with the Agency under the provisions of ORS 192.345(3), and after complying with all legal requirements.

This department will not release information originated by any other agency (ORS 192.311 et seq). Individuals requesting this information shall be referred to the originating agency.

## 806.6 SECURITY OF PROTECTED INFORMATION

The Police Chief will select a member of the Agency to oversee the security of protected information.

The responsibilities of this position include but are not limited to:

(a) Developing and maintaining security practices, procedures, and training.

(b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents including computer attacks.

(d) Tracking, documenting, and reporting all breach of security incidents to the Police Chief and appropriate authorities.

### 806.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

## 806.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

### 806.7.1 LEDS TRAINING

All members who operate a terminal to access the LEDS network shall complete a LEDS System Training Guide at a level consistent with the member's duties. Each member who operates a terminal to access LEDS must be re-certified by the Agency every two years (OAR 257-015-0050).

# Appendix B
**Unmanned Aerial System**

Policy **605**

City of Sherwood Police Department
Sherwood PD OR Policy Manual

# Unmanned Aerial System

## 605.1 PURPOSE AND SCOPE
The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval and dissemination of images and data captured by the UAS.

605.1.1 DEFINITIONS
Definitions related to this policy include:

**Unmanned Aerial System (UAS)** - An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached systems designed for gathering information through imaging, recording, or any other means.

## 605.2 POLICY
A UAS may be utilized to enhance the department's mission of protecting lives and property when other means and resources are not available or are less effective. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations.

## 605.3 PRIVACY
The use of the UAS potentially involves privacy considerations. Absent a warrant or exigent circumstances, operators and observers shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure). Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions can include, for example, deactivating or turning imaging devices away from such areas or persons during UAS operations.

## 605.4 PROGRAM COORDINATOR
The Police Chief will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations, and best practices and will have the following additional responsibilities:

- Coordinating the FAA Certificate of Waiver or Authorization (COA) application process and ensuring that the COA is current (OAR 738-080-0045), and/or coordinating compliance with FAA Part 107 Remote Pilot Certificate, as appropriate for department operations.
- Ensuring that all authorized operators and required observers have completed all required FAA and department-approved training in the operation, applicable laws, policies, and procedures regarding use of the UAS.
- Developing uniform protocols for submission and evaluation of requests to deploy a UAS, including urgent requests made during ongoing or emerging incidents.

  Deployment of a UAS shall require written authorization of the Police Chief or the authorized designee, depending on the type of mission.
- Coordinating the completion of the FAA Emergency Operation Request Form in emergency situations, as applicable (e.g., natural disasters, search and rescue, emergency situations to safeguard human life).
- Developing protocols for conducting criminal investigations involving a UAS, including documentation of time spent monitoring a subject.
- Implementing a system for public notification of UAS deployment.
- Developing operational protocols governing the deployment and operation of a UAS including but not limited to safety oversight, use of visual observers, establishment of lost link procedures, and secure communication with air traffic control facilities.
- Developing a protocol for fully documenting all missions.
- Developing a UAS inspection, maintenance, and record-keeping protocol to ensure continuing airworthiness of a UAS, up to and including its overhaul or life limits.
- Developing protocols to ensure that all data intended to be used as evidence is accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, authenticity certificates, and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.
- Developing protocols that ensure retention and purge periods are maintained in accordance with established records retention schedules.
- Facilitating law enforcement access to images and data captured by the UAS.
- Recommending program enhancements, particularly regarding safety and information security.
- Ensuring that established protocols are followed by monitoring and providing periodic reports on the program to the Police Chief.
- Ensuring that the UAS is registered with the Oregon Department of Aviation (ORS 837.360).

- Developing protocols for storage, security, and access to data collected by the UAS (ORS 837.362).
- Developing protocols if a third party is used for the storage of data, including handling, security, and access to the data by the third party (ORS 837.362).
- Developing protocols for disclosing data collected by the UAS through intergovernmental agreements (ORS 837.362).
- Publishing the department policies and procedures regarding the use, storage (including third party storage), accessing, sharing, and retention of data collected by the UAS, including the text of ORS 192.345 on the department website or other publicly accessible system (ORS 837.362).
- Maintaining familiarity with FAA regulatory standards, state laws and regulations, and local ordinances regarding the operations of a UAS.

## 605.5 USE OF UAS

Only authorized operators who have completed the required training shall be permitted to operate the UAS.

Use of vision enhancement technology (e.g., thermal and other imaging equipment not generally available to the public) is permissible in viewing areas only where there is no protectable privacy interest or when in compliance with a search warrant or court order. In all other instances, legal counsel should be consulted.

UAS operations should only be conducted consistent with FAA regulations.

The UAS shall only be operated by the Agency (ORS 837.320; ORS 837.330; ORS 837.335):

(a) Pursuant to a valid warrant authorizing its use.

(b) When there is probable cause to believe that a person has committed a crime, is committing a crime, or about to commit a crime, and exigent circumstances exist that make it unreasonable to obtain a warrant authorizing the use.

(c) With written consent of an individual for the purpose of acquiring information about the individual or the individual's property.

(d) As part of search and rescue activities, as defined in ORS 404.200.

(e) When assisting an individual in an emergency if there is a reasonable belief that there is an imminent threat to the life and safety of the individual.

1. A report shall be prepared documenting the factual basis for the belief.
2. Within 48 hours of the emergency, a sworn statement shall be filed with the circuit court describing the nature of the emergency and the need for the use of the UAS.

(f) During a state of emergency declared by the Governor, if:

1. The UAS is used for preserving public safety, protecting property, or conducting surveillance that will be used to assess and evaluate environmental or weather-related damage, erosion, or contamination.

2. The UAS is operated only in the geographical area specified in the Governor's proclamation.

(g) For the purpose of reconstructing a crime scene or accident scene, or a similar physical assessment that is related to a specific investigation, as provided by ORS 837.340.

(h) For the purpose of training in the use and acquisition of information, as provided in ORS 837.345.

## 605.6 PROHIBITED USE

The UAS video surveillance equipment shall not be used:

- To conduct random surveillance activities.
- To target a person based solely on actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.
- To harass, intimidate, or discriminate against any individual or group.
- To conduct personal business of any type.

The UAS shall not be weaponized (ORS 837.365).

The UAS shall not be used in any way that causes interference with an aircraft that is in the air, taking off, or landing (ORS 837.374).

## 605.7 RETENTION OF UAS DATA

Data collected by the UAS shall be retained as provided in the established records retention schedule (ORS 837.362).

## 605.8 REPORTING

The Records Section supervisor shall ensure that an annual report is provided to the Oregon Department of Aviation that summarizes the frequency of UAS use and the purpose for the use, and indicates how the public can access the department's policies and procedures regarding the use of data resulting from the use of UAS as required by ORS 837.360.

# Appendix C

**Preflight Checklist**

- Airspace – Check Aloft app for flight location and submit LAANC request if needed.
- Weather Conditions – Visually check weather conditions and if needed check Aloft. Determine if you are comfortable flying in such conditions.
- Visual Observer – If applicable select a unit for the visual observer role and explain their role.
- Take Off and Landing Zone – Visually inspect landing zone for debris, obstacles, and potential hazards in the area that may interfere with takeoff and landing.
- Compass Calibration – Check compass to ensure it doesn't need calibration.
- Controller, GPS & Signal Strength – Ensure controller is fully charged and is connecting to satellites at/above minimum (15+). Proper placement of antennas to ensure it's connected to the drone.
- Drone – Ensure parts are in good working condition. Remote controller, flight battery, and tablet are charged to an acceptable level. Ensure propellers are securely mounted onto the motors, and the motors can start and function normally.
- Gimbal and Camera – Remove gimbal protectors and ensure there is no foreign object stuck to the camera, and that gimbal can rotate freely before powering it on.
- UAV Health Management System – Ensure the app is functioning correctly and aircraft's firmware has no system errors. Ensure proper flight mode is selected, and all sections are green and say "Normal".