OPRD Policy # IT.071:

Use and Storage of Data Collected by Unmanned Aircraft Systems

Authorized:	Date:
Lisa Sumption, Director	06/01/2017

INTRODUCTION & OVERVIEW

Summary Policy Statement

OPRD uses unmanned aerial vehicles as a safe and cost-effective way to replace existing aerial surveys performed by contract services. Data collected by small unmanned aerial systems (sUAS) replace or supplement both contract service data and ground surveys in accordance with OPRD's mission to protect and enhance Oregon's special places. This policy establishes expectations for the use, storage, accessing, sharing, and retention of data resulting from the operation of sUAS.

Purpose:

The purpose of this policy is to establish protocols and set standards to protect information assets resulting from the collection of data within the OPRD sUAS Program. The Program is maintained by the Information Technology section and exists to provide service across the agency.

Background

Oregon statute requires public bodies to establish policy for the acquisition, maintenance, storage, sharing, and destruction of data acquired by sUAS. This policy is part of a series of policies related to information security and complies with statute and direction from DAS on data standards/security. Information security has become an increasingly important topic of conversation in today's world. Whether it is government operations or the private sector, completed work must frequently rely heavily on the use of technology. While technology has provided great efficiencies, it has also brought reasons for caution and a need for close monitoring and regulation. Security breaches and misuse of information and business equipment takes many forms, from privacy violations, stolen identity and financial fraud, to reduced productivity and damaged equipment. Generally, dealing with these instances has a cost and continues to cost businesses, government entities and private citizens a significant amount of money every year.

In Oregon, there are several laws and policies that govern this topic, as outlined in the Authority section. OPRD's Chief Information Officer developed this policy to clarify statewide laws and policies, detail OPRD's policy for protecting information assets, and provide relevant guidance for agency employees.

Goals

The goals of this policy are to ensure that OPRD employees understand the following:

- OPRD employees have the responsibility to keep information and technology assets secure;
- Security is consistently applied for employees' use of information resources and provides a framework for tracking information assets; and
- OPRD must remain in compliance with both statewide security policies and State law regarding the use of and any data collected with sUAS by public bodies.

Scope

Applicability: This policy applies to all information assets, whether paper-based, held within data bases, mobile based, general portable or permanent electronic files, documents, worksheets, geospatial, engineering drawings, photography, video or graphical in nature.
Audience: This policy is directed to all OPRD employees and volunteers whether or not they utilize electronic information assets.

Authority

The authority for this policy is established in ORS 837.300 to 837.900 Use of Unmanned Aircraft Systems and ORS192.501 generally Oregon's record retention laws. Statute addresses the use, operation and storage of resultant data acquired by sUAS. OPRD authority to develop policy on major programs under its control is represented in Gen.010 Development and Management Policy.

Related Policies & Procedures

This policy is related to the following OPRD policies:

- IS 030.010 PR Information Asset classification, defining the risk levels for classifying information assets.

- IT-070 Use of sUAS by OPRD and Contractors

POLICY PROVISIONS

Definitions

Asset: Anything that has value to the organization.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Security: Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Risk: The likelihood of a threat agent taking advantage of vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.

Security Policy: Documentation that describes senior management's directives toward the role that security plays within the organization. It provides a framework within which an organization establishes needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and organization commitment managing risks.

Small Unmanned Aircraft System (UAS): Means an unmanned flying machine, commonly known as a drone, and its associated elements, including communication links and the components that control the machine.(ORS 837.300)

Public body- has the meaning given that term in ORS 174.109

Policy Statements

General

1) Data collected by sUAS may be used to count, classify, observe and measure cultural, natural, physical resources and assets.

2) OPRD will hold data collected in a secure and safe manner in accordance to Information Security Policies, and will provide data via public access requests as applicable to public records laws. Providing data classified as level 3 or 4 must have overriding need and be approved by the Director or designee.

3) Data collected by sUAS will be retained by OPRD to the standards set forth by the Secretary of State for OPRD's handling and retention of information.

4) Data collected by sUAS will be primarily used for internal projects by OPRD, and/or for reference to cultural, natural, physical resources and assets. Data will occasionally be included in publicly available websites for consumption by the general public, at the sole discretion of OPRD. Technical data shared with other entities will be established by formal agreement. In the event that data is made available via third party storage, it will be vetted by OPRD as generally available and informational data. Third party providers shall be under the same obligations as OPRD to securely store and manage data as established by formal agreement.

5) Data collected by sUAS will be managed and stored centrally under the supervision of the sUAS Coordinator and the OPRD CIO. Data collected by sUAS shall have an accompanying collection report which includes at minimum the following: date of collection, name of sUAS pilot in command, OPRD responsible party if different than PIC, latitude and longitude of the center of the data collection, general description of the type of data collected, network location of data. Copies of collection reports shall be submitted to OPRD sUAS Coordinator.

Security Review

OPRD sUAS data owners will perform annual reviews of the general security of the data collected, including retention. Reviews shall be verified by OPRD sUAS Coordinator.

Exceptions

None.

Roles and Responsibilities

Administrator, Business and TechnologySolutions Division: Approve policy and subsequent reviews. Approve process for granting, changing and terminating access to information assets for employees at the various stages of their employment, from initial hire, to voluntary changes and termination.

Chief Information Officer: Educate management on the provisions of this policy; provide assistance with how to use the relevant portions for policy users, be it staff, manager or both; monitor the use of the policy, review user comments and track changes in State direction; revise the policy when needed.

sUAS Coordinator: Collate internal use reports and provide annual summary to Oregon Department of Aviation. Manage storage of OPRD sUAS data and maintain public access to OPRD sUAS policy.

Failure to Comply

Failure to comply with this policy may be cause for disciplinary action up to an including dismissal.

ADMINISTRATION

Owner: BATS Division

Approval: OPRD Director
Contact for questions:
Trygve Larson, CIO
725 Summer St NE
Suite C
Salem, Or. 97301
trygve.larson@oregon.gov

Dates:

First approval date: June 1, 2017
Effective date: June 1, 2017
Revision schedule: yearly
Next revision date: June 1, 2018

Feedback:

Your comments are extremely important to improving the effectiveness of this policy. If you would like to comment on the provisions of this policy, you may do so by e-mailing policy.feedback@oregon.gov. To ensure your comments are received without delay, please list the policy number and name in your e-mail's subject. Your comments will be reviewed during the policy revisions process and may result in changes to the policy.