Oregon Department of Fish & Wildlife (ODFW) Volunteer Program Policy

Title:	Acceptable Use of State Information Assets by Volunteers	**Policy #:**	Vol 500_02
Applicability	Volunteers who access the department's network or network services or who use or have access to ODFW information assets		
Reference(s)	DAS Policy 10-040-01 Statewide Employee Training ISD Policy 610_01 Acceptable Use of State Information Assets ISD Policy 610_03 Mobile Communication Devices ISD Policy 610_04 Information Technology Lifecycle ISD Policy 620_01 Information Asset Classification ISD Policy 620_02 Transporting Information Assets ISD Policy 630_01 Security of Information Systems ISD Policy 630_02 Portable Data Storage ISD Policy 640_01 Cloud Computing MRD Policy 710_09_002 Use and Storage of Data Collected by Unmanned Aircraft Systems Vol Policy 500_01 Code of Conduct		
Effective Date:	May 1, 2022	**Approved:**	

I. Purpose:

This policy establishes the appropriate and acceptable use of state information assets (e.g., computers, peripherals, portable computing devices, software, data, network, and other technology) for all volunteers.

II. Policy:

A. It is the policy of the Oregon Department of Fish and Wildlife to provide access to information systems and computing devices for conducting business in support of the agency's mission, goals, and objectives. All data, computing devices, or systems are for the exclusive use of state business except as otherwise exempted by agency policy. It is the duty of all Volunteers to protect state information assets entrusted to their use from accidental or purposeful disclosure, modification, or loss. Volunteers that use state information assets are responsible for complying with the provisions of this policy, supporting policies, procedures, and practices. (Ref: ISD Policy 610_01 Acceptable Use of State Information Assets).

1. Mobile Communication Devices

    a. Mobile Computing Devices (MCD) are considered an extension of the agency computer network and therefore subject to the existing policies and procedures as other computing devices. (Ref: ISD Policy 610_03, Mobile Communication Devices).

2. Information Technology Lifecycle

    a. The Information Systems Division (ISD) will establish and periodically update technology standards including serviceable lifecycle expectations for common technology used by the agency. (Ref: ISD Policy 610-04, Information Technology Lifecycle).

3. Information Asset Classification

    a. All information assets owned or in custodial care by ODFW will be classified and managed based on its confidentiality and sensitivity requirements. Proper levels of security will be implemented to protect information assets according to its relative classification. (Ref: ISD Policy 620_01, Information Asset Classification).

4. Transporting Information Assets

    a. ODFW has established minimum safeguards to protect information assets throughout the delivery/transport cycle. Volunteers are responsible to assure appropriate security controls are utilized in the protection of the information assets (physical or electronic) during preparation, transportation, receiving, and final delivery. Controls are intended to prevent unauthorized disclosure, misuse, loss, corruption, or unintended modification. (Ref: ISD Policy 620_02, Transporting Information Assets).

5. Security of Information Systems

    a. It is the responsibility of every Volunteer to protect the confidentiality, integrity, and availability of ODFW data and technology assets entrusted to their use. (Ref: ISD Policy 630_01, Security of Information Systems).

6. Portable Data Storage

    a. Due to their small size and high capacity, portable data storage devices and the information they contain can be easily compromised, lost, or stolen. Volunteers are expected to take the necessary precautions to prevent unauthorized access when in use, stored, in transit, or disposed. (Ref: ISD Policy 630_02, Portable Data Storage).

7. Cloud Computing

    a. All cloud solutions will be operated and maintained in a manner that supports the mission of the agency and in compliance with state and agency policies and procedures as if the service were provided on state owned/operated systems. At all times, cloud solutions must be properly licensed, operationally sustainable, and secure. (Ref: ISD Policy 640_01 Cloud Computing).

8. Use of Storage of Data Collected by Unmanned Aircraft Systems

    a. Data collected by Unmanned Aircraft Systems (UAS) will be used to observe, count, classify, and measure fish, wildlife, habitat, and users of fish and wildlife to further the Department's mission. (Ref: MRD Policy 710_09_002, Use and Storage of Data Collected by Unmanned Aircraft Systems).

9. Training Requirements

    a. Volunteers whose Volunteer Service Description includes access to any of the following shall complete the OSCIO Security Training on an annual basis. ODFW has granted a policy exception to all other Volunteers. (Ref: DAS Policy 10-040-01 Statewide Employee Training)

        i. ODFW Network of VPN

        ii. Internet enabled ODFW devices, either assigned or provided for use

        iii. ODFW Systems that require measures for security and privacy of information

        iv. Unsupervised ODFW Facilities

ACKNOWLEDGEMENT

Click here to acknowledge receipt and understanding of the Acceptable Use of Information System Assets by Volunteers Policy