OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	**Cloud Computing**	**ISD_640_01**
Supersedes:	None	
Applicability:	All state employees (their agents), volunteers, vendors and contractors, including those affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objectives.	
Reference:	State policy 107-004-150 Cloud Computing	
Effective Date:	**March1, 2020**	**Approved:**

I. PURPOSE

This policy establishes the standards and expectations to procure, download, establish, maintain, secure, and audit the use of cloud software, cloud services, and cloud solutions. The cloud offers great opportunities to redefine and modernize our business but only if done so strategically and with forethought. State policy requires all cloud software, services, and solutions must be approved prior to implementation to analyze and document benefits, costs, and risks to the state in addition to assessing the readiness of a cloud application/vendor to deliver a solution where assets are appropriately secured and protected.

II. DEFINITIONS

A. **Cloud Computing (Also known as Cloud Services):** Agency data created, processed, or stored (uploaded) on resources that are not provided directly by the agency or State of Oregon. A model for delivering information technology services or applications (free or fee based) in which resources are retrieved from the Internet through web-based tools, rather than from a user's PC or from agency network servers. Data and software applications are stored or hosted from remote data servers.

Examples of Cloud Services include, but are not limited to, ELS, Google Docs, Sales Force, WiFoo, Xhibit, Watercraft Inspection & Decontamination (WID), In-Reach, OnXMaps, internet email, on-line collaboration, and any data storage external to ODFW systems.

B. **Information Asset:** Any data, application, computer, peripheral, portable device, or other technology used to store, transport, modify, display, or report information that has value to the organization regardless of its physical form or characteristics.

C. **User:** All state employees (and their agent), volunteers, vendors, and contractors, including those users affiliated with third parties who access state information assets, and all others

authorized to use state information technology for the purpose of accomplishing the state's business objectives.

III. POLICY

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 practices as if the service was provided on state owned/operated systems. At all times cloud solutions must be properly licensed, operationally sustainable, and secure.

A. Applicability

This policy collectively applies to all cloud applications and services including those obtained with portable devices, smart phones, or solutions provided as part of a contract service.

B. Compliance

Users are responsible to fully comply with cloud policy and procedures to avoid significant risk associated with external hosting of data and applications in terms of security, account management, licensing, retention, interoperability, and audit.

C. Business Considerations

Cloud solutions can present significant business challenges such as managing account access controls as an enterprise technology or securely integrating data and services functioning as isolated and discrete services. Consideration must be given how future business needs may create demands for data and service integration and how these demands will be met agency, state, or partner organizations. Contractual terms may be necessary to ensure data and services are available for future integration through Application Programming Interfaces (APIs) or Active Directory (AD) integrations.

D. Pre-Deployment/Acquisition

Prior to contracting, purchase, acquiring, or use, a cloud readiness assessment must be approved by the Information Systems Division, and as applicable Enterprise Information Services. These documents identify the potential business impacts and risks that includes confidentiality, business continuity, service management, incident management, change management, records management, intellectual property rights, data ownership, audits, and controls.

The selection of products and use of cloud computing technology or services must comply with all applicable laws, policies, procedures, and standards including without limitation: privacy laws and regulations, statewide and agency specific IT security policies, internal audit controls, risk management standards, and records management standards.

Prior to contracting or selection of a cloud service or application, it is highly recommended to obtain a pre-assessment to gain an adequate understanding of process, criteria, and potential impacts to the project planning.

Smart phone applications are considered a form of cloud services/application and also require an assessment/certification prior to use.

E. Vendor Supplied Cloud Services, Applications, Tools

As established through contract and approved within the scope of services described in the approved cloud workbook for a project, ODFW employees are permitted to use cloud-based services that are provided by the contract vendor for the administration, reporting, or testing the services provided. By example, a cloud-based bug tracking tool, project management tool, or common data repository.

F. Access and Audit

All cloud solutions must have a designated access coordinator that will ensure access rights are appropriately assigned and managed in alignment with agency security principle of least rights privilege. User accounts must be audited on a regular basis, typically monthly, to promptly remove access to any user that has been reassigned to other duties, employment has been terminated or is no longer in need of the cloud service.

The Information Systems Division will fill the role of designated access coordinator whenever access rights can be established that allow centralized account management or can be done so through automation.

G. Sole Source Information

At no time shall users allow the cloud service to become the sole source of agency data or information without the expressed written approval and documented authorization within the completed cloud workbook. Such sole source requires approval by both the agency CIO and Enterprise Information Services.

Cloud services may contain replicate (copy) or comingled data (derived information) as long as original information is maintained on agency computer resources. Cloud may also contain temporary or transactional information that has no significant impact to agency business as documented within the cloud readiness assessment form.

H. Procedures

Complete a service request ticket to have a review completed for any cloud software or solution prior to any procurement, contract, or use. Contact ISD for additional details or information.

IV. POLICY GROUP

This policy is part of a suite of Information Technology policies that collectively sets the expectations and use of computing devices and related technology, and falls under the principle policy ISD_610_01 'Acceptable Use of Information Systems'.