OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	Cloud Computing	ISD_640_01
Supersedes:	ISD_640_01 Cloud Computing dated March 1, 2020	
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:	Jan 1, 2024	**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 has great potential to redefine and modernize our business but only if done so strategically and with forethought.

II. DEFINITIONS

A. **Authoritative Source:** A repository or system that is the official informational reference considered to be highly reliable and most accurate source of information.

B. **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.

C. **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.

D. **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 hosted directly on state owned/operated systems. 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 that is appropriately secured and protected. 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 included as bundled services with portable devices, smart phones, or solutions provided as part of a contract service.

B. Risk Compliance

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

C. Legal Compliance

Cloud applications 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.

D. Integration and Security

Integration account authentication and security protocols are required to the maximum extent possible and as appropriate for the cloud application or service. This includes but not limited to Application Programming Interfaces (APIs), Active Directory (AD) integrations, and Multifactor Authentication (MFA).

E. Pre-Deployment/Acquisition

Prior to contracting, purchase, or use, a cloud readiness assessment must be completed by the user and approved by the Information Systems Division, and as applicable Enterprise Information Services per state policy 107-004-150 Cloud and Hosted Systems. 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.

Completing a Contract Service Request (CSR), participating in a competitive procurement process, and completing associated contractual agreements may also be required prior to use of a cloud application or service. See ASD policy for additional information.

F. **Vendor Supplied Cloud Services, Applications, Tools**

As established through a vender contract and approved within the scope of services described in the approved cloud workbook for a project, users are permitted to use contractor provided cloud-based services or tools that are licensed and utilized by the contract vendor for the administration, reporting, or testing of their services. By example, a contract vendor may utilize their own cloud-based bug tracking tool or project management tool.

G. **Authoritative (sole) Source / Replication**

At no time shall the cloud service become the only authoritative source of agency information or data without the pre-approval by the agency CIO and Enterprise Information Services (EIS) as documented within the state required cloud readiness workbook.

Cloud services may contain replicate (copy) or comingled data (derived information) as long as original information is maintained on agency computer resources. Cloud services may also contain temporary or transactional information that has no significant impact to agency business if lost or unavailable.

H. **Access and Audit**

All cloud solutions must have a designated access coordinator that will ensure user 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, unless access the cloud solution is network integrated (see section Integration and Security) and occurs automatically. This is necessary to remove access rights from any user that is no longer employed by ODFW, reassigned other duties, 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 Active Directory or other automation.

I. **New Cloud Service Requests**

State policy 107-004-150 'Cloud and Hosted Systems' requires agencies to assess the readiness and risks prior to implementation of each cloud service. A cloud workbook must be completed to evaluate criteria based on statewide and agency risk thresholds.

This review and approval process can vary significantly based on the risk, complexity, cost, and type of service. Each of these elements have thresholds requiring additional information or oversight. At a minimum, state policy requires ISD to review the request for technical and security purposes. ISD has delegated authority to provide final approval for requests with low risk, cost, and complexity.

Requests that exceed agency oversight thresholds may be required to submit a Contract Service Request (CSR), participating in a competitive procurement process, and complete associated contractual agreements. These requests may also be subject to governance prioritization for agency resources.

Requests that exceed state oversight thresholds will require further review by DAS/EIS analysts to ensure the hosted system meets all state requirements.

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 main policy ISD_610_01 'Acceptable Use of Information Systems'.