

RFP 170-4420-25 Compliance Management Solution Attachment K

Status **Active** PolicyStat ID **15949311**



**OREGON
STATE
TREASURY**

Origination 01/2018

Last 10/2024

Approved

Last Revised 07/2020

Next Review 10/2026

Owner **Dr. Donald
Johnson: Chief
Information
Security Officer**

Policy Area **Information
Technology**

IT 407: Cloud Computing Policy

INTRODUCTION & OVERVIEW

Summary Policy Statement

This policy establishes limitations and requirements in the use of cloud storing and sharing services.

Purpose and Goals

The purpose of this policy is to ensure that OST data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing and file sharing, for this purpose, is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with OST such as, but not limited to, social networking applications, file storage, and content hosting.

Applicability

This policy applies to all persons accessing and using third-party services capable of storing or transmitting OST data, all consultants, agents, contractors and any parties who are contractually bound to handle data produced by OST, and in accordance with OST's contractual agreements and obligations.

This policy pertains to all cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

POLICY PROVISIONS

Policy Statements

All cloud service providers that OST intends to engage with must meet minimum information security protections. Cloud services shall:

1. Be vetted and approved by IT prior to use. A list of vetted cloud services is maintained by IT.
2. Encrypt data while stored and during transmission.
3. Store OST data entirely in the United States.
4. Use multi-factor authentication to authenticate to the cloud service and must integrate with OST's Single Sign-On architecture.
5. Send security access logs to OST's security information and event management system (SIEM).
6. Provide the ability to easily export OST data upon termination of contract or use.
7. Develop a responsibility matrix chart (RACI) in collaboration with OST IT.
8. Perform regular security scans and audits. Annual SSAE 16 SOC 2 Type 2 or similar is strongly recommended.
9. Comply with all applicable laws, policies procedures and standards including without limitation: privacy laws and regulations, statewide security standards and OST-specific policies.
10. Meet state public records laws and with all other applicable federal and state statutes, rules, and policies.
11. Contracts must ensure ownership of and rights to intellectual property and data are appropriately retained.
12. Must include terms and conditions required by Department of Justice (DOJ) in order for the contract to be approved for legal sufficiency according to ORS 291.047. For external cloud computing services that require users to agree to terms of service agreements, such agreements must be approved by DOJ.
13. Document service level agreements, business continuity and disaster recovery requirements in the proposed contract.
14. Carry cyber risk insurance appropriate for the proposed transaction.

Exceptions

Exceptions to this policy must be reviewed and approved by IT Management.

Failure to Comply

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

PROCEDURES and FORMS

OSCI Statewide Policy on Cloud Computing 107-004-150

Oregon Public Records laws – ORS 192.410 to 192.505

Public Contract Approval by Attorney General ORS 291.047

ADMINISTRATION

Review

Biennial

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 the Policy Analyst. 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.

Approval Signatures

Step Description

Approver

Date

	Jerry Walker: CIO/Director of Information Technology	10/2024
IT Managers	Brenda Gibson: CTO Chief Technology Officer	10/2024
IT Managers	Sebrina Gridley: Technical Service Delivery Manager	07/2024
IT Managers	Adam Burt: Application Development Manager	06/2024
Information Technology CISO	Dr. Donald Johnson: Chief Information Security Officer	05/2024