ENTERPRISE information services

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

STATEWIDE POLICY

	NUMBER 107-004-150	**SUPERSEDES** Policy #107-004-150 | (2019)
	EFFECTIVE DATE **REVIEWED DATE**	**PAGE NUMBER** Pages 1 of 4
DIVISION Enterprise Information Services (State CIO)	**REFERENCE** ORS 276A.206, 276A.300, 276A.303 Cloud Security Procedure: 107-004-150_PR	
POLICY OWNER Cyber Security Services		
SUBJECT Cloud Security	**APPROVED SIGNATURE** Terrence Woods, State Chief Information Officer	

PURPOSE

This policy establishes requirements for state agencies to:

- Identify, analyze and consider risks with cloud services before contracting or renewing a contract for such service.
- Conduct planning and define requirements to ensure that state information assets and data are appropriately protected when adopting a cloud service.
- Assess the security capability of a cloud service provider to ensure delivery of a solution that meets the state's requirements.

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.300, and includes any board, commission, department, division or office within the Oregon Executive Branch. The following agencies and board are excluded:

- Secretary of State
- State Treasurer
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery
- State Board of Higher Education or any public university listed in ORS 352.002

ATTACHMENT

- Attachment A: Cloud Checklist

DEFINITIONS

Cloud service: an internet-based computing solution that provides shared processing resources, applications and access to data on demand, made available to state agencies through various contracting models. This includes services provided by another state agency external to the organization.

Cloud service provider (CSP): the entity providing a cloud service.

Infrastructure as a service (IaaS): the capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (National Institute of Standards and Technology (NIST) Computer Security Resource Center Glossary)

Some examples may include virtual machines, storage accounts, and networks provisioned with cloud services brokered by Data Center Services (DCS).

Platform as a service (PaaS): to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (NIST Computer Security Resource Center Glossary)

Some examples may include database as a service, containers, K*S, lambdas and firewalls as a service provisioned within cloud services provided by third parties or brokered by DCS.

Software as a service (SaaS): using a provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST Computer Security Resource Center Glossary)

Some examples may include Workday, Microsoft 365 (M365), all M365 including Power Platform (Power Apps, Power Automate, Power BI, Power Pages, Power Virtual Agents also knows as Copilot Studio), and Fabric. Although Microsoft's Power Platform exhibits some characteristics of PaaS, it is considered a SaaS

GENERAL INFORMATION

This policy addresses the security of all applicable state agencies' technology, systems, data and networks implemented in public, private, hybrid and multi-cloud infrastructures, plus all applicable state agencies' IT assets implemented in cloud services as defined by Enterprise Information Services (EIS).

The selection and use of cloud services must comply with all applicable laws, and comply with, meet or exceed policies, procedures and standards, including without limitation:

- Privacy laws and regulations
- Statewide and agency-specific IT security policies, plans, and standards
- Internal audit controls, risk management standards
- Records management standards
- Applicable statewide policies and procedures

Contracting and Agreements of Cloud Services

Before and during the process of contracting for a cloud service, the agency must appropriately manage the associated risks. Planning should be started as soon as a cloud service is considered and must be carried out with diligence and rigor appropriate to the size, business impacts and risk of the proposed solution.

While in the process of acquiring new or renewed cloud services, agencies must complete and submit the Cloud Checklist (attachment A), as part of their review of a cloud service provider's ability to meet security and baseline needs. EIS Cyber Security Services (CSS) will review the completed Cloud Checklist and provide requirements and recommendations.

Security of Cloud Services and Data

Required security baselines include but are not limited to the Statewide IT Control Standards, Information Security Program Plan, and regulatory, legislative, and policy-based requirements. Additionally, for DCS-brokered services, the appropriate Center for Internet Security (CIS) benchmark(s) for the cloud solution platform will be implemented.

Agencies will:

- Adhere to statewide policies on IT investment.
- Utilize the Cloud Checklist as a detailed in this policy.
- Ensure appropriate controls are in place to meet agency needs, applicable legal and regulatory cybersecurity controls, and statewide policies, standards and requirements.

Note: Cloud services providers with current GovRAMP moderate or higher authorization and with CSS having visibility to the GovRAMP artifacts will not be required to complete the Cloud Checklist

Agency submission of the Cloud Checklist to EIS constitutes acknowledgement and acceptance of risk by the agency. The agency is solely responsible for ensuring the appropriate technology manger(s), chief information officer, deputy chief information officer, senior manager(s), director(s), agency head or other necessary leadership are involved and aware.

EIS CSS will:

- Ensure cloud security policies and associated procedures are established in compliance with this policy.
- Provide security standards and guidance for agencies on cloud environments and solutions, and information safeguarding. This includes the GovRAMP authorization program.
- Review completed Cloud Checklists and provide any requirements and recommendations.
- Document, create and maintain security controls for state-managed cloud environments to align with state security standards, guidelines and requirements.
- Design, deploy and manage security-focused resources for state-managed cloud environments to align with state security standards, guidelines and requirements.
- Ensure third party cloud solutions are reviewed and meet state security requirements before giving security authorization to integration with state resources.

EIS DCS will:

- Provide IT standards, requirements and guidance for agencies on DCS-managed IaaS and PaaS, and identify services in alignment with state security standards, guidelines and requirements.
- Ensure alignment with state security standards, guidelines and requirements for DCS-managed cloud environment.
- Ensure third-party cloud solution integrations are reviewed and meet DCS requirements before giving DCS authorization for integrations with state resources.

- Collaborate with other EIS programs, Department of Administrative Services State Procurement Services and Department of Justice, as broker and managed service provider for PaaS, IaaS, and DCS-managed SaaS solutions, to develop processes that incorporate security review and ensure adherence to state security and IT standards, guidance and requirements.

Assistant State Chief Information Officers will:

- Consult with agencies for alignment with EIS Strategic Framework and agency IT strategic plan.