ENTERPRISE information services

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES STATEWIDE PROCEDURE	**NUMBER** 107-004-150_PR	**SUPERSEDES** Policy #107-004-150 | (2019)
	EFFECTIVE DATE **REVIEWED DATE**	**PAGE NUMBER** Pages 1 of 2
DIVISION Enterprise Information Services (State CIO)	**REFERENCE** ORS 276A.206, 276A.300 Cloud Security: 107-004-150	
POLICY OWNER Cyber Security Services		
SUBJECT Cloud Security	**APPROVED SIGNATURE** Terrence Woods, State Chief Information Officer	

PURPOSE

This procedure outlines tasks of Executive Branch agencies to comply with Statewide Policy 107-004-150, Cloud Security, when considering cloud services before contracting such service, and to ensure state information assets and data are appropriately protected when adopting and using a cloud service.

APPLICABILITY

Refer to the Cloud Security Policy (107-004-150) for applicability of this procedure.

ATTACHMENT

- Cloud Checklist, attachment A to Statewide Policy 107-004-150.

DEFINITIONS

Refer to the Cloud Security Policy 107-004-150.

PROCEDURE

RESPONSIBILITY	STEP	ACTION
Agency	1	Identifies a cloud service for consideration.
	2	Consult with Assistant State Chief Information Officer for alignment with Enterprise Information Services (EIS) Strategic Framework and agency IT strategic plan.

RESPONSIBILITY	STEP	ACTION
	3	Prior to awarding a contract during the procurement process, work with the cloud service provider to complete the cloud checklist. Submit completed cloud checklist at ESO.INFO@das.oregon.gov
EIS Cyber Security Services (CSS)	4	Review the completed cloud checklist, and other related information as needed, for associated security risks and IT controls. Provide requirements and recommendations. Notify Data Center Services (DCS) if the request involves brokered or managed infrastructure as a service (IaaS) or platform as a service) PaaS services.
EIS DCS	5	If the request involves brokered or managed IaaS or PaaS services, prepares for the required changes and estimate the timeline for brokerage or managed services.
Agency	6	Ensure additional needs outside of this policy and procedure for the acquisition or renewal of cloud service(s) are being met. This may include, but is not limited to, engagement with EIS and other entities to meet security requirements, implementation requirements, contractual and procurement needs, and additional review and collaboration.
	7	Ensure cloud service provider adopts and implements appropriate controls and benchmarks to each cloud environment before state information assets are hosted in the cloud service provider environment.
	8	Work with CSS throughout the engagement, including contract development and finalization.