Cloud Computing Standard

Introduction

The OMES Information Security cloud computing strategy is based on a hybrid environment, which leverages the existing external cloud when possible and selectively utilizes the on-premises environment when beneficial. Using the on-premises environment, also referred to as a private cloud, allows the State of Oklahoma to leverage existing investments in infrastructure and provide a stable and secure environment.

OMES IS adheres to the National Institute of Standards of Technology guidelines for cloud computing strategy as a standard.

Purpose

This document outlines best practices for using cloud computing services to support the processing, sharing, storage and management of state information.

Definitions

Cloud computing – a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage and services) that can be rapidly provisioned and released with minimal effort or service provider interaction.

Standard

The implementation preference for cloud computing for state agencies is Microsoft Azure Commercial and Amazon Web Services Commercial. MAC and AWS cloud infrastructures comply with the highest industry standards of data security for remote hosted contents and are FedRAMP certified. In addition, MAC and AWS allow for OMES IS to select the data geography region that best fits the requirements of the data being utilized.

The State of Oklahoma recognizes there are laws and regulations for data types that require Microsoft Azure Government or AWS commercial. Similar to MAC, MAG has the same comprehensive security controls in place. Whereas each of the cloud environments (MAC and MAG) are assessed and authorized at the FedRAMP High impact level, MAG provides an additional layer of protection through contractual commitments for storing customer data in the United States. In addition, support personnel are screened resources that reside in the United States. Should support be needed after hours, the screened support personnel may reside outside of the United States.

While AWS provides a unique infrastructure that negates the ability of AWS employees to access underlying data, please note that MAG cloud infrastructure is required when CJIS data is stored or accessed. MAG (as opposed to MAC) is also required when a data geography region cannot be configured by OMES IS, but regulatory compliance requires such ability.

If the usage is related to the states data platform, then Google Cloud Platform will be used.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- Microsoft Products Available by Region.
- Azure Geographies.
- NIST Computer Security Resource Center – Cloud Computing.
- CJIS Security Policy Version 5.9.
- FTI 1075.
- AWS Services in Scope by Compliance Program.
- Google Cloud Supported Products by Compliance Program.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 01/25/2021	**Review cycle:** Annual
Last revised: 01/12/2024	**Last Reviewed:** 1/30/2024
Approved by: Joe McIntosh, Chief Information Officer	