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 Information Services adheres to the National Institute of Standards and Technology (NIST) 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 primary implementation preference for cloud computing for state agencies is Microsoft Azure Commercial. MAC cloud infrastructures comply with the highest industry standards of data security for remote hosted contents and is FedRAMP certified. In addition, MAC allows 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 which require Microsoft Azure Government. Similar to MAC, MAG has the same comprehensive security controls in place. Whereas both cloud environments 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. It should be noted that MAG cloud infrastructure is required when CJI and FTI data is being stored and/or accessed, as well as when a data geography region cannot be configured by OMES IS, but regulatory compliance requires such ability.

References

- Microsoft Products Available by Region.
- Azure Geographies.
- NIST Computer Security Resource Center – Cloud Computing.
- CJIS Security Policy Version 5.9.
- FTI 1075.