Offshore Data Storage Standard

Introduction
Data is a valuable asset to business and government, and as such, it is imperative that state data be stored securely. Offshore data storage is a popular industry option, particularly for cloud storage. However, because other countries and regions use different guidelines, international laws and regulations, offshore storage options may be less secure and more vulnerable to security incidents than data stored within the United States. Offshore data storage also increases the risk that data stored offshore could be subject to the sovereign control of another country. To reduce the security and jurisdictional concerns inherent to offshore data storage, OMES requires state data to remain within the boundaries of the U.S.

Purpose
This document establishes the standard for state data to be stored within the boundaries of the U.S.

Definitions
- Offshore – A location that is outside the physical borders of the U.S.
- Follow-the-sun model – IT support model that utilizes global resources to provide 24/7 support for IT services and solutions.

Standard
OMES requires all state data to be hosted, stored, processed, transmitted, accessed and disposed of by approved vendors within the boundaries of the U.S.

State agency systems and data shall not be accessible from outside the physical boundaries of the U.S. unless granted an exception approval following the Security Exception Standard or otherwise following the International Travel Standard (which is limited to employees).

Vendors/suppliers may be allowed to provide a follow-the-sun service model in order to provide 24/7 support for IT services, cloud management, incident response, troubleshooting, customer support, and application development for services and solutions utilized by state agencies.

Offshore support is only permitted on systems that use public data. Any regulated data, i.e. HIPAA, FERPA, CJI, etc., must be supported by onshore resources only. Vendors/suppliers are required to provide the list of countries services will be provided from in order to ensure no undue risk to state data and systems will be incurred.

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

- International Travel Standard.
- Security Exception Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 08/29/2022	**Review cycle:** Annual
Last revised: 02/11/2025	**Last reviewed:** 02/11/2025
Approved by: Dan Cronin, Chief Information Officer	