Email Protection Standard

Introduction

The State of Oklahoma must ensure integrity and accessibility of records, as well as secure sensitive state information that may be sent or received via email. Mass forwarding or auto-forwarding state emails poses a data security threat that can put employees, contractors and agencies at risk.

State employees and contractors are required to use state email accounts for state business. The use of personal email accounts to conduct state business is strictly prohibited.

Purpose

This document establishes expectations around protecting email. State of Oklahoma email accounts used to conduct state business require appropriate security, backup and records-retention measures to be in place. The state is obligated to ensure public records and sensitive information are protected appropriately.

Definitions

State email tenant – The environment managed, maintained and protected by the Office of Management and Enterprise Services which provides access to email services, instant messaging, online collaboration and virtual meetings.

Forwarding – Redirecting communications from the intended destination to another without the sender's knowledge.

Auto-forwarding email – Automatically directing all incoming messages to another destination.

Sensitive information – Any information protected by federal, state or local regulations or statute where loss, misuse, unauthorized access or modification thereof could adversely affect national or state interests or the conduct of federal/state programs or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (Privacy Act).

Standard

All state employees and officials must use the state email tenant for all state business including, but not limited to, activities in support of agency missions and job specific functions.

In order to protect sensitive and confidential state information, no request to forward state email to addresses outside of the state email tenant is allowed. Additionally, the following applies to state email.

- Any email containing sensitive information sent to an external party must be sent by secure email. Employees and contractors who fail to do so may be required to complete additional training. Repeat offenders may be referred to the agency's HR department and could result in loss of access.
- Oklahoma Cyber Command may block unsecure email when sensitive information is identified.
- The spam filter for the state automatically blocks messages with a high probability of being spam. End users are responsible for managing their spam filters through the Mimecast Personal Portal.

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

- Mimecast Toolkit.
- Mimecast Personal Portal.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 02/24/2022	**Review cycle:** Annual
Last revised: 02/24/2022	**Last reviewed:** 08/30/2023
Approved by: Joe McIntosh, Chief Information Officer	