OKLAHOMA
Office of Management
& Enterprise Services

Security Awareness Training Standard

Introduction

OMES IS is responsible for developing, implementing and maintaining a security awareness and education training plan for all state agencies. The plan documents the process for employee and contractor training, education and awareness, as well as ensures all state employees and contractors understand their role in protecting the confidentiality, integrity and availability of state data.

Purpose

This document establishes the security awareness training standard for the State of Oklahoma. The purpose of awareness presentations is to focus attention on security and are intended to promote an environment recognizing IT security concerns and responding accordingly.

Awareness relies on reaching broad audiences, whereas training is more formal, with a goal of building knowledge and skills to facilitate job performance. Effective IT security awareness presentations must be designed. Awareness presentations must be on-going, creative and motivational, with the objective of focusing attention so the learning will be incorporated into conscious decision-making.

Definitions

User – All State of Oklahoma employees, contractors, board members or other persons authorized to connect to the state network.

Security education and awareness training – Also known as SEAT, is used to educate employees and contractors on how to protect state assets and information systems.

Phishing simulation – An internal control testing methodology which stimulates a real-life phishing attempt. Pushed enterprise-wide to gather metrics on click rates/trends to better inform the focus of training efforts.

Standard

All users are required to complete OMES provided SEAT training annually unless required to do so more frequently due to IS departmental requirements or elevated access.

All state agencies are responsible for ensuring all staff members complete security awareness training.

Additionally, the state has an established cadence for facilitating phishing simulations. By providing simulated phishing exercises, the state can obtain a direct measurement of employee understanding, as well as progress in user behavior. Continuous email phishing assessments can be effective by indicating patterns of phishing vulnerabilities within a department and identifying further awareness training needs.

Any users who fail simulated exercises are required to complete additional training. Repeated failures may be referred to the agency’s HR department and could result in loss of access.

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.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 01/31/2021	**Review cycle:** Annually
Last revised: 05/16/2023	**Last reviewed:** 10/14/2024
Approved by: Joe McIntosh, Chief Information Officer	