OKLAHOMA
Office of Management
& Enterprise Services

SSL Inspection Standard

Introduction

To protect information transmitted over the Internet from interception and misuse by unauthorized parties, the data must be encrypted. Secure Sockets Layer technology encrypts data being sent over a connection, and that same data must be decrypted at its destination point. In order to improve network security posture, follow compliance guidelines and fulfill regulatory compliance framework, any SSL traffic destined for OMES resources must be decrypted and inspected.

Purpose

This document establishes the OMES standard to decrypt inbound SSL traffic on the state network.

Definitions

Secure Sockets Layer – A security protocol used for protecting private information during transmission via the Internet.

Standard

All SSL-encrypted inbound traffic to the OMES network must be decrypted and inspected upon offload. Any exceptions to this standard must be approved by OMES Cyber Command.

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

- Transport Layer Security Standard.
- NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.

This standard is subject to periodic review to ensure relevancy.

Effective date: 04/10/2023	**Review cycle:** Annual
Last revised: 04/10/2023	**Last reviewed:** 10/03/2024
Approved by: Joe McIntosh, Chief Information Officer	