Transport Layer Security Standard

Introduction
Transport Layer Security is an encryption protocol applied to data communications transmitted over the internet. OMES utilizes TLS 1.2 to protect all data transmitted on the state network but vulnerabilities with this version have been identified. A newer version, TLS 1.3, was released in 2018 with upgrades designed to address the vulnerabilities identified in TLS 1.2. OMES is poised to implement TLS 1.3 as the future standard for data communications transmitted over the state network, thus enabling OMES to mitigate the risk of compromised data communications on the state network.

Purpose
This document establishes TLS 1.2 as the current standard for protecting transmitted data.

Definitions
Transport Layer Security – An authentication and encryption protocol widely implemented in browsers and web servers.

Standard
The state standard for encryption and authentication of data transmitted on the state network is TLS 1.2 or later.

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

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 10/05/2022	**Review cycle:** Annual
Last revised: 10/05/2022	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	