Data Encryption Standard

Introduction
The State of Oklahoma utilizes digital certificates to confirm identity, secure communications and ensure the integrity of data transmissions. Certificates are used as a method of encryption for data while in transit, at rest and during processing.

Purpose
This document defines the authority, roles and requirements for data encryption within the state.

Definitions
Certificate – An authoritative certificate containing a public key that can encrypt or decrypt electronic messages, files, documents or data transmissions and establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing, protecting and escrowing the private component of the key pair associated with the encryption certificate.

Data in transit – Any type of information that is actively moving between systems, applications or locations.

Data at rest – Any type of information that is not actively moving from a device to a network (e.g., data stored on a hard drive, laptop, archive or mobile device).

Standard
Oklahoma Cyber Command is the state authority for encryption certificates. This authority includes tracking certificates, notifying owners when the expiration date is approaching and approving certificate requests. Oklahoma Cyber Command manages the state's certificate authority, tracks and processes new and renewal requests for the OMES infrastructure and applications teams, provides installation and configuration support when requested and supports OMES account representatives in certificate selection and billing inquiries.

Additionally, encryption must be used to protect the transmission and storage of state data. All data must be encrypted while in transit and while at rest. Full encryption is required for all state-issued devices.

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: 03/02/2022	**Review cycle:** Annual
Last revised: 10/21/2022	**Last reviewed:** 09/21/2023
Approved by: Joe McIntosh, Chief Information Officer	