OKLAHOMA
Office of Management
& Enterprise Services

Data Security Standard

Introduction

Data belonging to the State of Oklahoma must be managed properly to ensure data use is compliant with all applicable state and federal regulations, and that data on Oklahoma citizens is not misused or allowed to fall into the hands of malicious actors. Storage, encryption and secure transmission of data is of paramount importance and the integrity of state data must be preserved at all times.

Purpose

This document establishes requirements for protecting State of Oklahoma data and applies to the following:

- The proper storage, encryption, and transmission of state data.
  - *Data encryption.*
- The proper handling of removable storage, and media destruction procedures,
  - *Data storage.*
  - *Removable media*.
  - *Media disposal*.
- The principals of *least privilege/least functionality* to minimize state data exposure to only those use cases for which it is needed.

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).
- Offshore – A location that is outside the physical borders of the U.S.
- FIPS – Federal Information Processing Standards; Publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems of non-military government agencies and contractors.
- PII – Personal Identity Information; any information related to an identifiable person. Personal identity information includes Social Security numbers, tax identification numbers, bank account numbers, credit card numbers, personal health information (PHI) and drivers' license numbers.
- Removable media device – Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards. Examples include but are not limited to USB flash drives, external hard drives and external solid-state disk (SSD) drives.
- Sensitive data – Any data that includes PII, information deemed confidential by the nature of the agency's business, or information regulated by federal, state and local

regulations. Current and former state employee personal contact information, such as home phone numbers and addresses and information related to electronic communication devices are considered sensitive information by state statute.

- Media – Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Standard

Data encryption.

All state data must be encrypted while in transit and at rest. The primary method for data encryption is through the use of asymmetric key encryption, which uses security certificates to encrypt and decrypt data as needed. All security certificates for the State of Oklahoma are managed by Oklahoma Cyber Command, including acquisition, provisioning, renewals, and disposal.

Data storage.

All state data must be stored either on a server in the State Data Center, or on an approved cloud platform which limits data storage and access to the borders of the United States of America. No state data is to be stored in a data center, or on a cloud platform that uses offshore facilities, nor should offshore support personnel have access to live state data.

Offshore tech support is permitted under the following conditions:

- Offshore support resources are not permitted to have access to the production environment or to production/live data which is sensitive or subject to the State of Oklahoma or federal regulations.
- Offshore support resources can have access to dummy data on lower environments (e.g. development or test).
- No path to the production environment or data can exist for offshore support personnel, even if escorted (digitally or physically) by OMES IS personnel

Removable media.

As a general rule, removable media should not be used on State of Oklahoma devices because such devices are extremely easy to lose and do not support the same robust encryption safeguards that other storage media provide. There are cases, however, in which removable media is a valid option. In those cases, removable media which makes use of hardware-level encryption must be used. These devices must meet or exceed FIPS 140-2 encryption standards. A list of acceptable devices can be found on the Permitted Technologies list.

Media disposal.

It is crucial that authorized data destruction techniques be used for secure wiping of media, in compliance with NIST 800-88, Rev. 1, Guidelines for Media Sanitization, to ensure comprehensive eradication and deter data recovery.

Additional controls:

- Only authorized personnel/vendors should be involved in media disposal activities.
- Non-disclosure statements are required of vendors providing off-site media disposal services.
- Media destruction should be certified by a media disposal vendor or OMES surplus.
- Detailed disposal records must be maintained, documenting the media type, the disposal method employed and the accountable party overseeing the disposal.

Least privilege/least functionality.
To ensure that state data is adequately protected, all hardware, software and user accounts must follow the principals of least privilege and least functionality. Put simply, this means that no system or user should have access rights to data or software for which they do not have an approved business need, and that systems and accounts should be built to do one thing only. As an example, if a process needs a service account to move files from location A to location B, and also to write new data into location C, two separate accounts should be created. One to move files from location A to location B, and one to write new files to location C. This approach minimizes the risk of any one account or system becoming compromised.

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

- National Institute of Standards and Technology.
- NIST SP 800-88 Guidelines for Media Sanitization.
- NIST SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC.
- NIST SP 800-171A Rev. 3, Assessing Security Requirements for Controlled Unclassified Information | CSRC.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 06/17/2025	**Review cycle:** Annual
Last revised: 06/17/2025	**Last reviewed:** 06/17/2025
Approved by: Dan Cronin, Chief Information Officer	