Removable Media Usage Standard

Introduction

Oklahoma Cyber Command is responsible for protecting state users, their managed devices, and connectivity to data and applications. Oklahoma Cyber Command's top priority is safeguarding the state's data and computer infrastructure against unauthorized data use, disclosure, modification, damage and loss.

Purpose

This document establishes acceptable use requirements for sharing, receiving or storing state data utilizing removable media devices.

Microsoft OneDrive is the preferred alternative to using any form of removable media device for sharing, receiving or storing state data. OneDrive for Business is provided to all state employees and contractors as the approved storage solution. OneDrive has been vetted for the protection of state data and users' privacy (Reference Workstation Data Storage Standard).

Definitions

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.

Standard

Oklahoma Cyber Command is required to provide information security services to all state agencies, as defined in Title 62 O.S. § 34.11.1, including establishment of data protection controls.

Unmanaged usage of removable media devices creates increased risk of sensitive data disclosure either inadvertently through loss or theft of the device or by purposeful data exfiltration. To assist in mitigating sensitive data disclosure risks, Oklahoma Cyber Command shall implement technological-based procedures to disallow regular usage of removable media devices not previously approved for use within our managed enterprise environment.

For a removable media device to receive regular usage approval:

- The device must be a state-owned asset. Personally owned devices shall not be utilized to share, receive or store state data.
- The device must be capable of hardware encryption that meets or exceeds applicable regulatory compliance requirements (generally FIPS 140-2, level 2 or 3 will cover the most stringent requirements).
- The device must internally contain and report an individual vendor/model/serial number which provides an inventory control mechanism.
- Vendor devices meeting this criterion are listed below. Please confer with Oklahoma Cyber Command for review and approval of comparable devices outside this list.
    - Secure Data.
    - Apricorn.
    - Data Locker.
    - Kanguru.

After each use-case for sharing, receiving or storing state data has been completed, data must be purged from the removable device in accordance with any and all applicable state and federal regulations.

Exceptions to removable media device regular usage approval must be requested with a documented business justification for CIO review.

It is the responsibility of Oklahoma Cyber Command to interpret, design, implement and manage required regulatory controls. Staff performing similar functions within state agencies must collaborate and coordinate all activities with Oklahoma Cyber Command and defer interpretation of regulations and final decisions/solutions to Oklahoma 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

- Workstation Data Standard.
- Oklahoma State Statute, Title 62.
- National Institute of Standards and Technology.

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

Effective date: 06/04/2024	**Review cycle:** Annual
Last revised: 06/07/2024	**Last reviewed:** 09/19/2024
Approved by: Joe McIntosh, Chief Information Officer	