Media Disposal Standard

Introduction
This document outlines the proper disposal of media to ensure confidential data, sensitive data and licensed software cannot be accessed by unintended persons.

Purpose
This standard establishes clear guidelines for the secure disposal of all forms of media containing sensitive information, with the aim of preventing unauthorized access and potential data breaches.

Definitions
- 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.
- Sensitive data – Confidential information that is stored, processed or managed by an organization that is confidential and only accessible to authorized users with proper permission, privilege or clearance to view.

Standard
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.

According to the Third-Party Cybersecurity Management Standard, the approved media disposal vendor must undergo routine managed assessments to identify any potential risk and ensure appropriate controls are in place to protect sensitive data.

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.

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

- Third-Party Cybersecurity Management Standard.
- NIST 800-88, Rev. 1, Guidelines for Media Sanitization.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 07/26/2024	**Review cycle:** Annual
Last revised: 07/26/2024	**Last reviewed:** 07/26/2024
Approved by: Joe McIntosh, Chief Information Officer	