Digital Forensics Standard

Introduction
As a state agency, it is important to have a digital forensics standard in place to protect and preserve digital evidence during investigations. This document establishes State of Oklahoma guidelines for digital forensics.

Purpose
This standard is meant to guide the practices and procedures of digital forensics analysts, ensuring that investigations are conducted systematically, ethically and in compliance with the law and State of Oklahoma policies.

Definitions
Digital forensics – Forensic science encompassing recovery, investigation, examination and analysis of material found in digital devices.

Standard
The following guidelines should be followed in digital forensic analysis:

- OMES Cybercommand must have identified the scope and purpose of digital forensics, to include supporting a cyber security incident and employee misconduct investigation. This should include the types of investigations the agency conducts and the types of digital evidence that may be collected.
- OMES CyberCommand must have established procedures/user guides for the acquisition and preservation of digital evidence. This includes developing guidelines for the collection, storage and transportation of digital evidence to ensure it is not compromised or altered. The guidelines should also outline the procedure for creating a chain of custody to maintain the integrity of the evidence.
- OMES CyberCommand must have guidelines for the analysis and interpretation of digital evidence: OMES has established guidelines for the tools and techniques used to analyze digital evidence, as well as guidelines for interpreting the results, including procedures for data recovery, data analysis and data interpretation.
- OMES CyberCommand must have procedures for the reporting of digital evidence. This includes guidelines for the creation of reports and the presentation of findings in court. The guidelines should ensure that the reports are accurate and complete and that they follow the legal requirements for the jurisdiction in which the investigation is taking place.
- OMES CyberCommand must have guidelines for the security of digital evidence. This includes guidelines for the protection of digital evidence from unauthorized access, theft or destruction. The guidelines should ensure that the digital evidence is stored in a secure location and that only authorized personnel have access to it.

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: 11/13/2023	**Review cycle:** Annual
Last revised: 11/13/2023	**Last reviewed:** 11/13/2023
Approved by: Joe McIntosh, Chief Information Officer	