Reporting Lost or Stolen Digital Asset Standard

Introduction
The loss or theft of digital assets poses a significant risk to the State of Oklahoma. This standard outlines procedures and protocols for addressing the loss or theft of digital assets.

Purpose
This standard applies to all employees, contractors and third-party vendors who have access to state digital assets.

Definitions
Digital asset – Any data, information or software stored electronically or in a digital format including computing devices, PCs, portable computers, mobile devices, tablets or any other device used to store data.

Loss – Unintentional misplacement or destruction of digital assets.

Theft – Unauthorized or illegal taking of digital assets.

Stakeholders – Individuals or entities directly involved in managing or safeguarding digital assets.

Standard
Time is of the essence when a digital asset is lost or stolen. Employees must report immediately upon identifying a device is lost, missing or stolen.

Employees must immediately notify their manager in the case of lost, missing or stolen digital state asset(s).

The employee must also contact the OMES Service Desk electronically at mailto:servicedesk@omes.ok.gov or by telephone at 866-521-2444 or 405-521-2444 to report the item missing, lost or stolen. Any item stolen or presumed stolen must have a police report filed with the local law enforcement agency. The police case number must be reported to the OMES Service desk within 24 hours of reporting the device stolen for the Cyber Command operations team report.

Upon receiving a report of a lost or stolen digital assets, Cyber Command will initiate an investigation to determine the cause and extent of the incident.

Recovery efforts will be made to recover the lost or stolen asset(s) through various means, including collaboration with law enforcement agencies.

Cyber Command will complete a detailed report of the incident including findings from the investigation, actions taken for mitigation, recovery efforts, and lessons learned.

Depending on the severity and impact of the incident, immediate actions may be taken to mitigate further loss or damage to digital assets. This may include changing credentials, wiping the device, and notifying additional stakeholders about the incident.

When required, the chief information security officer contacts the governor's office within 24 hours of the report.

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