System Logging, Reviews and Privacy Standard

Introduction
In order to appropriately protect State of Oklahoma information technology resources and systems, it is necessary for OMES to generate, store and analyze logs that record events occurring within state systems and networks.

Purpose
This document establishes an expectation of system logging and monitoring processes across state information technology resources.

Standard
Users of the state's information technology resources are placed on notice that all computer systems maintain audit logs and/or file logs within the computer, and user information is backed up periodically. Information collected and stored may include, but is not limited to, user identification, date and time of the session, software used/accessed, files used/accessed, internet use and access, when requested and deemed necessary.

OMES reserves the right to view or scan any file or software stored on the computer or passing through the network and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as malware) or to audit the use of state resources. For example, analysis of audit files may indicate why a particular data file is being erased, when it was erased and what user account erased it.

Users should be aware information transmitted via the Internet may be intercepted by others. Accordingly, the privacy of electronic mail, voicemail and similar data should not be presumed.

With regard to all information system data, users should also be aware that the state's officers and employees, are subject to the provisions of the Oklahoma Open Records Act, 51 Oklahoma Statutes § 24A.1, et seq.

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: 04/07/2022	**Review cycle:** Annually
Last revised: 04/07/2022	**Last reviewed:** 07/14/2023
Approved by: Joe McIntosh, Chief Information Officer	