Log Aggregation Standard

Introduction
As our information technology environments increase in complexity and our organizations deploy an increasing number of applications and infrastructure in public and hybrid cloud environments, there is a growing need to maintain central control of application security and performance through log aggregation.

Purpose
To set a standard for log aggregation, including the tools to be used.

Standard
Anything that produces logs that can be aggregated, should be aggregated to the OMES standard tools for log aggregation.

The state standard tool for log aggregation of applications is Splunk, including Splunk Cloud**.**

Other tools besides Splunk may be used for log aggregation, review and scanning, but Splunk is the state standard for applications and must be used for any new application created after this standard has been made effective and likewise, any new device that has log data that is not a web or software application should aggregate their logs.

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
https://www.sumologic.com/glossary/log-aggregation/

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

Effective date: 07/27/2022	**Review cycle:** Annual
Last revised: 05/09/2022	**Last reviewed:** 12/06/2024
Approved by: Joe McIntosh, Chief Information Officer	