OKLAHOMA
Office of Management
& Enterprise Services

Application Software Support Standard

Introduction

The State of Oklahoma agencies and personnel have a responsibility to maintain vendor-supported software across all agencies to ensure the safety and security of software, systems and data. Software development life cycles vary across applications and vendors. However, all software eventually becomes unsupported. OMES IS is committed to ensuring the state maintains an up-to-date software portfolio to reduce the cost and risk inherent in managing unsupported software applications.

Purpose

The purpose of this standard is to outline the acceptable use and life cycle of application software. Each agency within the state requires application software to meet government business processes and provide services to the citizens of Oklahoma. Application software support procedures define a consistent process for managing the software life cycle and minimizing incompatibilities and reducing support cost to OMES and other state agencies.

Definitions

Supported software – Software for which there is commercial or vendor support options, including updates, upgrades, security patches and technical support services within two major version releases.

Unsupported software – Software for which the vendor no longer provides patches, updates or other technical support services.

Security assessment – The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

Standard

- Application software includes enterprise applications, custom applications, commercial off-the-shelf applications, legacy applications and all related software such as operating systems, virtualization, database, etc.
- Application software used on production systems must be supported software as defined above.
- OMES IS and agency management have the responsibility to enforce the use of supported software.
- Application software must undergo a security assessment prior to production deployment to determine and document potential vulnerabilities, weaknesses, risks or threats, and then work with the production team to mitigate those findings.

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: 10/12/2020	**Review cycle:** Annual
Last revised: 12/1/2023	**Last reviewed:** 12/1/2023
Approved by: Joe McIntosh, Chief Information Officer	