Permitted Technology Standard

Introduction
The State of Oklahoma has a responsibility to deliver and monitor IT systems, applications and data entrusted to it by its citizens. The Office of Management and Enterprise Services (OMES) carefully reviews technology and makes recommendations for continued use, disuse or bans on its use on state devices.

Purpose
This standard establishes technology or applications specifically permitted, used or downloaded on all state-owned data and devices, including laptops, desktops and mobile phones/tablets.

Definitions
- Application – A program that performs a specific business function.
- IoT – Internet of Things; a network of interrelated devices that connect and exchange data with other IoT devices and the cloud.
- Network devices – A device used to connect computer systems together to transfer resources or files. Examples include Wi-Fi access point, switch, router, etc.
- Storage – A purpose-built server used for storing, accessing, securing and managing digital data, files and services over a shared network or through the internet.
- Whitelisted – A cybersecurity strategy allowing only pre-approved or trusted entities to access a system or network.

Standard
The State of Oklahoma maintains a list of technologies permitted for use and/or download on any state-owned device or network. State-owned data may also be input into software or solutions included on this list.

Permitted Technology List.

All software and applications are not specifically referenced on the Permitted Technology List but assumed permissible based on the following:

1. Any whitelisted software in the state's privileged access management (PAM) platform.
2. Hardware listed on the Computer Ordering Widget (COW).

OMES continuously evaluates new and existing software and technology to ensure they integrate with other systems and continue to be the best solution in a changing and diverse work environment. Any new software or technology must be thoroughly vetted and approved by OMES Cyber Command to ensure the technology does not pose any risk to state-owned data or devices prior to usage on any state-owned device. State agencies may request a technology review by submitting a service request through the Service Portal requesting a Project and IT Approval Initiation Request.

OMES is committed to providing access to next-generation technology to state agencies and employees. We appreciate your cooperation in maintaining the security, compliance, and performance of our systems. Should you have any questions or concerns regarding this policy, feel free to reach out to the Information Services division at OMES.

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
- OMES Policies and Standards.
- Account Management Standard.
- Service Portal Project and IT Approval Initiation Request (PIR).
- Computer Ordering Widget.

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

Effective date: 6/30/2025	**Review cycle:** Annual
Last revised: 6/30/2025	**Last reviewed:** 6/30/2025
Approved by: Dan Cronin, Chief Information Officer	