IT Contractor Requirements Standard

Introduction
OMES IS is responsible for the IT onboarding process for State of Oklahoma employees and contractors. To support this effort, as well as promote consistency, the following standard has been established for the onboarding of contractors.

Purpose
This document outlines the standards for onboarding contract employees to ensure a consistent onboarding process.

Definitions
Least privilege – A security best practice to limit user privileges to only have access to what they need to perform their tasks and no more.

Standard
Any supplier accessing, processing, transmitting or storing state data must have their internal security controls appropriately evaluated and undergo a third-party risk assessment as defined in the Third-Party Cybersecurity Management Standard.

Agencies must ensure contractors comply with state policies, procedures and standards. Regardless of procurement method, prior to establishing a contractual relationship Oklahoma Cyber Command must evaluate contractors and/or organizations for potential security risks. Contracts or agreements, which may specify additional security requirements, must be completed and signed before a contractor is granted privileges for access to, or provisioning of, state information or resources.

Agencies negotiating, administering or managing contracts must ensure contractors comply with all applicable state policies, procedures, standards and with the terms specified in the applicable contract(s).

An OMES IS service division manager must be identified as an account sponsor. The service division manager is responsible for initiating the onboarding process.

Naming standards for contractors are in place to ease recognition of contract resources.

Contractors shall employ rule of least privileges. Additionally, contractor accounts shall be monitored by Customer Success – Provisioning to ensure utilization. Any account not using the system for 60 days will be disabled. After remaining in a disabled state for 30 days, the account will be offboarded for non-use. Semi-annual audits of contractor accounts will be provided to the contractor point of contact.

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
- Third-Party Cybersecurity Management Standard.
- Background Check Standard.
- Security Awareness Training Standard.

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

Effective date: 01/31/2022	**Review cycle:** Annual
Last revised: 10/17/2024	**Last reviewed:** 10/17/2024
Approved by: Aleta Seaman, Interim Chief Information Officer	