

## **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.

### **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 Risk 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 tower manager must be identified as an account sponsor. The service tower 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 access is limited to 90 days. Prior to expiration, the account sponsor is notified by Customer Success – Provisioning. It is the account sponsor's responsibility to request an extension. Extension requests submitted by a contractor will not be approved.

### **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 Risk Management Standard.](#)
- [Background Check Standard.](#)
- [Security Awareness Training Standard.](#)

### Revision history

This standard is subject to periodic review to ensure relevancy.

<b>Effective date:</b> 01/31/2022	<b>Review cycle:</b> Annual
<b>Last revised:</b> 07/27/2023	<b>Last reviewed:</b> 07/27/2023
<b>Approved by:</b> Joe McIntosh, Chief Information Officer	