Contractor Requirements Standard

Introduction

OMES Information Services is responsible for onboarding processes for State of Oklahoma employees, contractors and affiliates. To support this effort, as well as promote consistency, the following standard has been established for affiliate and contractor onboarding.

Purpose

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

Definitions

- Affiliate – worker who is not a state employee but serves in a supporting role to a state agency's mission, typically at the county, local or municipality level.
- Contractor - worker with economic independence who is in business for themselves but has been hired by the state to perform a particular function or produce a desired product.
- DSR - Decentralized Security Representative. The executive director of each agency delegates a DSR and delegates the security representative portion of his/her duties to a DSR. The DSR's authority comes solely from the executive director, who approved him/her to be the DSR. The DSR is acting on behalf of the executive director.
- 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.
- Naming standard – set of guidelines for naming entities, files, or variables to ensure consistency, clarity, and organization.
- Point of contact – designated person serving as the central coordinator regarding a specific project, activity or client relationship.
- User ID - unique login ID assigned to each user of state systems.

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 Supplier Chain Security Standard.

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).

Contractor and affiliate account creations and terminations must be DSR approved and manually submitted for processing via the OMES IS ticketing system.

An account sponsor holding DSR level authority must be present for each contractor account and serve as the point of contact for the contractor/affiliate.

The account point of contact is responsible for ensuring full compliance of contractor/affiliate accounts, including oversight, adherence to least privilege requirements, and timely offboarding in accordance with established standards.

Affiliate/contractor user ID naming standards for contractors are in place to ease recognition of contract resources.

Affiliate/contractor accounts shall be reviewed by the account point of contact semi-annually. The report will be provided by Cyber Command-Identity and Access Management.

For IT affiliates and contractors, the following additional requirements apply:

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

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 ensure efficient, secure, and cost-effective delivery of essential public services, all state agency IT purchases and projects must receive central approval. This allows the Chief Information Officer to evaluate agency needs and capabilities, strengthen data protection and security, and streamline and consolidate systems to reduce costs for taxpayers.

References

- Background Check Standard.
- Data Security Standard.
- Naming Convention Standard
- Security Awareness Training Standard.
- Supply Chain Security Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 05/11/2026	**Review cycle:** Annual
Last revised: 05/11/2026	**Last reviewed:** 05/11/2026
Approved by: Dan Cronin, Chief Information Officer	