# Identity Management Standard

## Introduction

User accounts are the only legitimate method by which OMES information systems may be accessed. OMES Information Services actively manages user accounts to prevent illegitimate use of state information systems. The use of authorization, identification and authentication controls ensure that only known users make use of state systems. Without these controls, the potential exists for information systems to be accessed illicitly, and the security of those information systems could be compromised.

## Purpose

This document defines the types of user accounts managed by OMES IS.

## 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.

Decentralized security representative (DSR) – individual, designated by the head of the agency, who is authorized to approve requests for their agency and state resources including creation of new user IDs, modification of user access and termination of user access.

Disabled account – inactive account requiring approval from an agency's DSR to enable.

Employee – worker who is economically dependent on the business of the employer.

Expired account – elapsed account for a contractor that has exceeded the configured expiration date.

Locked-out account – account that is blocked from user access and requires the OMES Service Desk to unlock (e.g. password expiration or a user incorrectly entering a password too many times).

Terminated account – User ID for an inactive affiliate, contractor or employee that has been disabled and had all permissions removed.

User ID – unique login ID assigned to each user of state systems.

## Standard

- OMES IS ensures all users (affiliates, contractors and employees) are issued a user ID whose activity is uniquely identifiable on IT systems and is established through an authentication mechanism.
- Prior to user access modification, DSR approval shall be obtained and approved access shall be granted with least privilege.
- Enterprise systems are provisioned access by roles approved by the agency and system owner when applicable. Examples include PeopleSoft Financials and Workday@OK.

- Generic accounts are not permitted without CIO approval obtained through an exception request. Generic accounts have additional controls in place for accountability and a periodic review for their applicability.
- Access for new user ID access (onboarding) is requested via the OMES IS ticketing system and must be approved by the DSR.
- Access termination requests for departed employees (offboarding) must be submitted by the user's agency at the time of separation of employment and is requested via the OMES IS ticketing system.
- Contractor accounts shall be reviewed by the owning agency semi-annually to verify continued access is required.
- User IDs not using the system for 60 days are verified against agency leave of absence reports prior to being disabled. Following a 30-day period of being disabled, the account is offboarded. Reactivation of the account requires an onboarding ticket to be submitted.
- Offboarded accounts are archived after a period of 30 days.
- To ensure proper access and continuity of business, individual user accounts shall not be used for shared resources, such as email or calendars. A dedicated resource for team or group activities must be requested.
- OMES employees are entitled to a single email account within the OMES mail domain regardless of their number of accounts within state systems.

**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:** 08/08/2023 | **Review cycle:** Annual |
| **Last revised:** 02/05/2025 | **Last reviewed:** 02/05/2025 |
| **Approved by:** Dan Cronin, Chief Information Officer | |