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. OMES IS utilizes Azure Active Directory to centralize account/identity management.

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.

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.

Disabled account – Inactive account requiring approval from an agency’s Decentralized Security Representative to enable.

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 – Inactive account for an employee or contractor who is no longer employed by the state.

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

Standard
OMES IS requires all users (internal, external and temporary) and their activity on IT systems be uniquely identifiable and that access is established through an authentication mechanism. All users of state systems have a uniquely identifiable user account.

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.

<table>
<thead>
<tr>
<th>Effective date: 08/29/2022</th>
<th>Review cycle: Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last revised: 08/29/2022</td>
<td>Last reviewed: 08/29/2022</td>
</tr>
<tr>
<td>Approved by: Jerry Moore, Chief Information Officer</td>
<td></td>
</tr>
</tbody>
</table>