Administrator Account Standard

Introduction

Pursuant to 62 O.S. §§ 34.11.1 and 34.12, OMES Information Services is responsible to direct the development, implementation and management of appropriate standards, policies and procedures to ensure success of state information technology initiatives and to establish and enforce minimum mandatory standards for information security and internal controls.

Such authority and responsibility are critical to the mission of OMES IS established therein. Accordingly, this standard applies to all State of Oklahoma employees, wherever located.

The consolidation of information technology infrastructure, data and computer systems presents unique possibilities and challenges for the State of Oklahoma. As a result of consolidation, advancements and an ever-evolving information ecosystem, new approaches to cybersecurity are required. The impact on citizens, the economy of Oklahoma and the nation depend on the cybersecurity posture of the state's IT infrastructure and computer systems. Attacks such as malicious code attacks, directed attacks by hackers and foreign governments, Advanced Persistent Threats, criminal enterprise, espionage and employee misconduct have advanced to the realm of technically proficient attackers and those with the motivation to succeed at all costs.

Purpose

This document establishes the requirements for administrator rights for state employees.

Definitions

- 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.
- Elevated privileges – A state in which a user account or process is granted higher access rights than a standard user
- Least function – A security best practice in which a server or system is configured with only the software, components and access rights to do a single task.
- 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

OMES does not allow for administrator access by users or super users. A user may request an exception; however, only OMES IS employees are eligible for elevated privileges.

When users are granted an administrator account, these additional responsibilities apply.

- All requests for administrator or elevated account privileges must be approved by an appropriate DSR.
- Administrator account permissions must be configured with least privilege.
- Administrator accounts shall not be used to browse the web (unless directly for the correction or facilitation of assigned work duties).

- Administrator accounts must not be used as a normal login for daily systems use. Additionally, the account shall be used only for items that require administrative access to correct issues or resolve problems.
- Administrator accounts shall not be used to change or modify any portion of the systems to bypass or circumvent security controls and all usage as an administrator account must be in accordance with this standard, as well as all federal, state and local laws.
- Administrator accounts shall not be used to install unapproved software on state-owned assets and must follow current established procedures for permission to install software through the OMES Service Desk.
- Administrator accounts shall not be used to install personal applications on state-owned assets – free software is not free. The tracking and usage taken from the systems violates state confidentiality and privacy laws and could lead to a compromise of state and federal data.
- Administrator account passwords must comply with the following requirements:
    - Avoid reusing or recycling old passwords. A new password cannot be the same as the previous 24.
    - Administrator account passwords shall not match the password of the individual's standard account.
    - Passwords must be a minimum length of 15 characters.
    - Passwords must include at least one lowercase letter, uppercase letter, numeral and special character.
    - Administrator accounts passwords must be changed at least every 60 days.
    - Administrators must utilize a strong two-factor authentication hardware token.

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

- Background Check Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 10/21/2013	**Review cycle:** Annual
Last revised: 03/31/2026	**Last reviewed:** 03/31/2026
Approved by: Dan Cronin, Chief Information Officer	