Service Account Standard

Introduction

The State of Oklahoma recognizes the importance of maintaining secure and reliable service accounts to protect sensitive information and ensure efficient access to authorized individuals. This standard outlines the requirements and guidelines for managing service accounts across all state agencies, departments and entities.

Purpose

This document defines the guidelines for the creation and use of service accounts managed by OMES IS.

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.
- Generic account – An account in a network domain used to represent a computer or device on the network. These accounts are used to authenticate and authorize access to network resources such as servers, printers and files. They typically have limited access rights, as they are not intended to be used by human users. Instead, they are used by services and applications to connect to network resources on behalf of the computer or device.
- 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.
- Service account – A special type of account used by a service or application to interact with the operating system. It is a local account created on a computer when a service or application is installed and is used to run that service or application. Service accounts are often used to provide security for services and applications, as they can be given the minimum amount of permissions necessary to perform their tasks, preventing unauthorized access to the system.
- User ID – unique login ID assigned to each user of state systems.

Standard

This standard applies to all service accounts used within the State of Oklahoma's information technology infrastructure, including, but not limited to, system accounts, application accounts and service-specific accounts.

Account creation and approval.

- All service accounts must be approved by OMES Cyber Command - Cyber Operations and created by Cyber Command - Identity and Access Management, following a formal request submitted via the OMES IS ticket system containing information to identify the business need and justification for the account creation.

- Account requests should be submitted through a Decentralized Security Representative (DSR) designated by the state's IT governance authority.
- Approval for account creation must be granted by the respective system or application owner and the designated IT security authority.

Account management.

- Service accounts should be assigned with unique and non-predictable in accordance with naming conventions.
- Passwords for service accounts must adhere to the state's password policy and be stored securely.
- Periodic password changes should be enforced for all service accounts, with a minimum password complexity requirement.
- Regular yearly reviews of service accounts should be conducted to identify and remove any unnecessary or unused accounts.
- Service accounts must be associated with an authorized owner responsible for their management and access.

Access controls and monitoring.

- Access to service accounts should be granted on a least-privilege basis, ensuring that only the necessary permissions are assigned.
- Access to service account credentials should be restricted to authorized individuals and stored securely using the State of Oklahoma OMES' encryption or secure key management systems.
- Audit logs for service accounts must be enabled and monitored regularly for any suspicious activities or unauthorized access attempts.
- Any detected security incidents related to service accounts should be reported to the appropriate incident response team or Cybercommand.

Account termination.

- When service accounts are no longer required, the accounts must be promptly deactivated or terminated. The account owner or their delegate must submit a ticket for processing by the OMES Identity and Access Management team via the OMES IS ticketing system.
- In the event the account owner's employment or responsibilities change, a request to transfer ownership must be submitted to the OMES Identity and Access Management team via the OMES IS ticketing system.
- Account termination should follow an established process that includes the removal of access permissions, disabling the account, and securely archiving or deleting any associated data.

Compliance

Insert 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

- Security Incident Response Standard.
- Account Management Standard.
- Application Security Standard.
- Identity Management 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:** 08/25/2026
Approved by: Dan Cronin, Chief Information Officer	