Account Management Standard

Introduction

The State of Oklahoma recognizes the importance of creating, configuring, monitoring and maintaining user accounts within the state's network while protecting sensitive information and ensuring efficient access to authorized individuals.

Pursuant to 62 O.S. §§ 34.11.1 and 34.12, OMES Information Services is responsible for directing 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.

Purpose

This document establishes account management requirements and guidelines for managing accounts across all state agencies, departments and entities and covers the following:

- Password requirements.
- Service account.
- Administrator/privileged account.
- IT contractor requirements.
- Remote employee.
- International travel.

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.
- Eligible employees – Employees who meet OMES standards for working remotely have authorization from their manager. Employees who are new parents or suffer from short-term/long-term disability may agree to longer periods of remote working with their manager and HR.
- 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.
- 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.
- Minimum data speed – The minimum data speed in megabits per second required for typical remote access and cloud application environments to perform essential job functions while protecting data integrity.
- Remote working – A permanent or temporary agreement between employees and managers to work from a non-office location for more than three days.
- 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.

- State device – Any state-owned asset including general storage devices, PCs, laptops/notebooks, mobile devices, tablets and any other devices used to store or access state data or infrastructure
- Telework – A flexible work arrangement where employees perform their job duties at an approved alternate worksite other than the location which the employee would otherwise work.

Standard

Password requirements.
The State of Oklahoma requires account passwords comply with the following minimum standards to help protect the integrity of state resources and data. All current and new accounts are subject to the following password requirements.

- Passwords must have a minimum length of eight characters.
- Passwords for elevated privileges to include access to highly regulated data sets (e.g., Federal tax information, criminal justice systems data, etc.) must be a minimum of 15 characters.
- Must contain at least one lower case letter, uppercase letter, numeral and special character.
- Passwords expire in a maximum of 90 days.
- Passwords are deactivated if not used for a period of 60 days.
- Passwords for elevated privileges are required to change passwords at least every 60 days.
- Password reuse is prohibited for 24 generations.
- The password requirements must be met where technically possible. In scenarios where existing technology does not support these standards an exception request to this standard is required.
- All passwords are treated as sensitive, confidential state information and therefore must be protected as such. Employees and contractors are responsible for keeping passwords secure and confidential. The following principles must be adhered to for creating and safeguarding passwords.
    - Passwords cannot be stored or shared in plain text.
    - Keep passwords confidential.
    - Do not keep a paper record of passwords.
    - Change passwords whenever there is any indication of possible system or password compromise.
    - Select quality passwords with a minimum length of eight characters which are:
        - Easy to remember.
        - Not based on anything easily guessed or obtained using person-related information (e.g., names, telephone numbers and dates of birth).
        - Free of consecutive identical characters or all-numeric or all-alphabetical groups.
    - Change passwords at regular intervals.
    - Avoid reusing old passwords or cycling old passwords.
    - Change temporary passwords at the first log-on.
    - Change default passwords for all devices at the first log-on.
    - Do not include passwords in any automated log-on process (e.g., stored in a macro or function key).
    - Do not share individual user passwords.

Service account.
Service account requirements apply 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 and created by Customer Success – Provisioning, following a formal request process that includes identifying the business need and a 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 usernames in compliance with OMES naming conventions to prevent unauthorized access attempts.
    - Passwords for service accounts must be a minimum of 25 characters long.
    - Passwords for service accounts must be rotated at least once per year.
    - Regular yearly reviews of service accounts should be conducted to identify and remove any unnecessary or unused accounts.
    - Service accounts must have 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.
    - Service accounts should be used for only one system or task and not on multiple systems. This facilitates password rotation without creating unacceptable risk of other systems being taken offline inadvertently.
    - 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 or when the account owner's employment or responsibilities change, the accounts must be promptly deactivated or terminated.
    - 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.
- Training and awareness.
    - Relevant training and awareness programs should be conducted periodically to educate personnel on the proper management and security of service accounts.
    - Authorized personnel responsible for managing service accounts should receive specialized training to ensure they understand the associated risks and best practices.

Administrator/privileged account.
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.
- Employees must not use the administrator account to browse the web (unless directly for the correction or facilitation of assigned work duties).
- Employees must not use the administrator account 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.
- Employees shall not use the administrator account 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.
- Employees shall not install unapproved software on state-owned assets and must follow current established procedures for permission to install software through the OMES Service Desk.
- Employees shall not 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.

IT contractor requirements.
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 Third-Party Cybersecurity Management Standard.

- Agencies must ensure contractors comply with state policies, procedures and standards. Regardless of procurement method, 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.
- 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).
- An OMES IS service division manager must be identified as an account sponsor. The service division manager is responsible for initiating the onboarding process.
- Naming standards for contractors are in place to ease recognition of contract resources.
- Contractors shall employ rule of least privileges. Additionally, contractor accounts shall be monitored by Customer Success – Provisioning to ensure utilization. Any account not using the system for 60 days will be disabled. After remaining in a disabled state for 30 days, the account will be offboarded for non-use. Semi-annual audits of contractor accounts will be provided to the contractor point of contact.

Remote employee.
Remote working is a permanent or temporary agreement between employees and managers to work from a non-office location for more than three days per week.

- Working from home for a maximum of [two days] or working from home certain days a week on a recurring basis are situations covered by our work-from-home policy.
- Remote working agreement.
  - Employees may work remotely on a permanent or temporary basis, if approved, with a properly executed and approved Telework Acknowledgment.
  - Permanent remote work employees should indicate their primary working address in a remote working agreement. This contract will also outline their responsibilities as remote employees.
- Remote working that works.

    - To ensure that employee performance will not suffer in remote work arrangements, we advise our remote employees to:
        - Choose a quiet and distraction-free working space.
        - Have an internet connection that's adequate for their job. The minimum bandwidth to successfully work from home is five (5) Mbps up/down.
        - Dedicate their full attention to their job duties during working hours.
        - Adhere to break and attendance schedules agreed upon with their manager.
        - Ensure their schedules overlap with those of their team members for as long as is necessary to complete their job duties effectively.
- Team members and managers should determine long-term and short-term goals. They should frequently meet (either online or in-person when possible) to discuss progress and results.
- Compliance with policies.
    - Remote employees must follow company's policies like their office-based colleagues. Examples of policies that all employees should abide by are:
        - Attendance.
        - Social media.
        - Confidentiality.
        - Data protection.
        - Employee Code of Conduct.
        - Anti-discrimination/Equal opportunity.
        - Dress code when meeting with customers or partners.
- All components of telework and remote access solutions should be secured against expected cyber threats as identified through threat models and include:
    - Never use personal devices to perform work, or save or transfer work, without management approval.
    - Enable zero touch deployment, where applicable.
    - Never use public Wi-Fi.
    - Utilize a password-secured network, if using wireless networking at home, using a hard to guess password.
    - Ensure ZScaler is installed on your computer and functioning properly.
    - Check for upgrades and patches regularly, implement as required.

International travel.
Traveling internationally involves special consideration to reduce the risk of theft of state assets and/or data. To this end, OMES discourages international travel with state devices. OMES prohibits international travel with state assets to countries on the US Department of State Travel Advisory List for level three and above and also prohibits access to state systems and networks while visiting those countries.

- When international travel is required, the approving manager must notify Oklahoma Cyber Command ten business days prior to the travel date to ensure appropriate security measures are in place. Oklahoma Cyber Command monitors all international connections into state infrastructure and will terminate any international connection that is not pre-approved

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
- US Department of State Travel Advisory List.
- Partnering with Information Services.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 05/13/2025	**Review cycle:** Annual
Last revised: 05/13/2025	**Last reviewed:** 05/13/2025
Approved by: Dan Cronin, Chief Information Officer	