Board Member Accounts Standard

Introduction
The Office of Management and Enterprise Services manages board member accounts to ensure state business is conducted via state resources to protect board members as well as uphold the Oklahoma Open Records Act.

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

Definitions
Board Member Account - A user account established for and used by a board member, either appointed or elected, and to be used to conduct state business.

Open Records Act – The Oklahoma Open Records Act, located at 51 O.S. § 24A.1 et seq. The ORA is an Oklahoma law requiring all records in the care, custody or control of public bodies and public officials in connection with the transaction of public business to be made available to the public, unless the records fall under an exception or exemption to the ORA.

Decentralized Security Representative – an individual designated by a state agency to approve user access, communicate security policies, procedures, guidelines and best practices to agency personnel and report on all deviations to security policies, procedures, guidelines and best practices.

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

Standard
This standard applies to all board member accounts used within the State of Oklahoma's information technology infrastructure.

Account creation and approval.

- All board member accounts will be created by Identity and Access Management following a formal onboarding process.
- Account requests are submitted through a Decentralized Security Representative designated by the state's IT governance authority.
- Board member accounts will be set up with an @ok.gov email address.

Account Management.

- Board member accounts will be assigned with unique and non-predictable user IDs to prevent unauthorized access attempts.
- Accounts will be set up on an expiration date schedule and shall be reviewed by the owning agency semi-annually.
- Passwords for board member accounts must adhere to the state's password policy and be stored securely.
- Periodic password changes will be enforced for all board member accounts with a minimum password complexity requirement.

Access controls and monitoring.

- Access to board member accounts will be granted on a least-privilege basis, ensuring that only the necessary permissions are assigned.
- Any detected security incidents related to board member accounts will be reported to the appropriate incident response team or Cyber Command.

Account termination.

- When board member 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 will follow an established process that includes the removal of access permissions, disabling the account and securely archiving or deleting any associated data.

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: 12/02/2025	**Review cycle:** Annual
Last revised: 11/21/2025	**Last reviewed:** 11/21/2025
Approved by: Dan Cronin, Chief Information Officer	