Acceptable Use Standard

Introduction

The State of Oklahoma establishes the acceptable behaviors and practices for using the state's technology and data resources to ensure integrity and accessibility as well as ensuring sensitive state information is protected.

Purpose

This standard establishes acceptable use behavior concerning the use of state's technology, data and resources. This standard applies to all employees, contractors and third-party vendors with access to the State of Oklahoma's systems, networks and data and covers the following:

- *Email protection and acceptable use*.
- *Network acceptable use*.
- *Information systems segregation*.

Definitions

- State email tenant – The environment managed, maintained and protected by the Office of Management and Enterprise Services which provides access to email services, instant messaging, online collaboration and virtual meetings.
- Forwarding – Redirecting communications from the intended destination to another without the sender's knowledge. Auto-forwarding involves automatically directing all incoming messages to another destination.
- Sensitive information – Any information protected by federal, state or local regulations or statute where loss, misuse, unauthorized access or modification thereof could adversely affect national or state interests or the conduct of federal/state programs or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (Privacy Act).

Standard

Email protection and acceptable use.

All state employees and officials must use the state email tenant for all state business including, but not limited to, activities in support of agency missions and job specific functions.

In order to protect sensitive and confidential state information, no request to forward state email to addresses outside of the state email tenant is allowed. Additionally, the following applies to state email.

Any email containing sensitive information sent to an external party must be sent by secure email. Employees and contractors who fail to do so may be required to complete additional training. Repeat offenders may be referred to the agency's HR department and could result in loss of access.

Oklahoma Cyber Command may block unsecure email when sensitive information is identified.

The spam filter for the state automatically blocks messages with a high probability of being spam. End users are responsible for managing their spam filters through the Mimecast Personal Portal.

Personal use of email is not permitted. Users shall have no expectation of privacy in any personal information sent, received or stored by a user using a state email account.

Users shall respect the purpose and charters of email distribution groups. It is the responsibility of any user of an email distribution group to determine the purpose before sending messages to the group or receiving messages from the group.

The state provides email services to support each agency's mission, and email is used as an official form of communication. All users are expected to demonstrate good taste and sensitivity to others in their communications. However, the state cannot protect individuals against the existence or receipt of material that may be offensive, and users are warned they may willingly or unwillingly come across, or be recipients of, material they find offensive. Individuals can report offensive material by emailing servicedesk@omes.ok.gov.

There is no privacy associated with the use of state email resources. Emails routed through the state email tenant are subject to the provisions of the Oklahoma Open Records Act. The state owns, and has right of access to, for any purpose, the contents of all computing information transmitted through or stored on its systems. The state may access and disclose any, or all, of the following:

- Data transmitted through or stored on its email and Internet access systems, regardless of the content of the data.
- Information related to the use of electronic communication.

Network acceptable use.

Access to networks owned or operated by the State of Oklahoma is provided to employees and contractors for use to support the mission of the state. Individuals who have access to state network resources are responsible for using those resources in an ethical and lawful manner.

Excessive or inappropriate usage of network resources may result in network access restriction, revocation of access privileges or further sanctions.

The State of Oklahoma Computer and Mobile Computing Device Usage policy for computer usage prohibits the use of its resources to access, create, transmit (send or receive), print or download material that is discriminatory, derogatory, defamatory, obscene, sexually explicit, offensive or harassing based on gender, race, religion, national origin, ancestry, age, disability, medical condition, sexual orientation or any other status protected by state and federal laws.

Authorized users of these network resources are only permitted to connect and utilize network devices that have been previously reviewed and approved by OMES Cyber Command. Given the potential for unapproved devices to cause network disruptions, service outages and reliability issues, users are prohibited from connecting such devices to the State of Oklahoma network. These prohibited devices include hubs, switches, repeaters, routers, network modems and wireless access points

Devices not approved for use on the State of Oklahoma network will have network access disabled and may be confiscated to ensure the stability and availability of the network.

Personal endpoint devices such as cell phones and laptops may only be connected to "oklahoma_open" Wi-Fi SSID. While these devices do not require prior review and approval from OMES Cyber Command, they are subject to the same rules regarding excessive or inappropriate usage.

Information systems segregation.
Information systems in the State of Oklahoma should have at a minimum, segregated development (Dev) and production (Prod) environments. Separation is essential to maintain security, integrity, operational stability and to prevent unauthorized access and accidental disruptions.

- Logical separation:
  - Implement network segmentation to ensure development and production environments are on different logical networks.
  - Use firewall rules and access control lists (ACLs) to enforce separation and prevent unauthorized traffic between development and production environments.
  - Use virtual private networks (VPNs) or secure tunnels to access production environments from development environments.
  - Development environments should not use production data wherever possible.
    - In rare cases where production data must be used, it must be de-identified to ensure sensitive information is not compromised and requires prior CIO approval.
- User access controls:
  - Use role-based access control (RBAC) to restrict access, based on job responsibilities.
  - Limit developers and operations team access to production environments. They should use automated deployment tools or pipelines to deploy code to production.
  - Implement just-in-time (JIT) access, where applicable, to limit access to operational environments for specific periods.
  - Ensure configuration management maintain separate configuration management repositories for development and production environments.
  - Ensure configuration settings and secrets (e.g., API keys, passwords) are securely stored and managed using the State of Oklahoma's secret management tools.
- Monitoring and logging:
  - Implement separate monitoring and logging infrastructures for development and production environments within the State of Oklahoma SIEM.
  - Monitor access logs and audit trails to detect and respond to unauthorized access attempts or anomalies.
- Training and awareness:
  - Conduct regular security training and awareness programs for development and operational teams.
  - Educate developers and operators about maintaining separate production and operations environments and following security best practices.
- Compliance and enforcement:
  - Compliance with this standard is mandatory for all teams involved in development and operations.
  - Regular audits and reviews should be conducted to ensure adherence to this standard.
  - Non-compliance may result in disciplinary actions as per the organization's policies.
- Responsibilities:
  - The IT security team is responsible for overseeing the implementation and enforcement of this standard.
  - Development and operational teams are responsible for adhering to these guidelines in their day-to-day activities.

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
- State of Oklahoma Computer and Mobile Computing Device Usage Policy.

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

Effective date: 07/02/2025	**Review cycle:** Annual
Last revised: 07/02/2025	**Last reviewed:** 07/02/2025
Approved by: Dan Cronin, Chief Information Officer	