OKLAHOMA
Office of Management
& Enterprise Services

Information Systems Segregation Standard

Introduction

This security standard aims to provide guidelines and best practices governing the separation of information system environments. At minimum, information systems in the State of Oklahoma should have segregated development (Dev) and production (Prod) environments. Separation is essential to maintain security, integrity, and operational stability and to prevent unauthorized access and accidental disruptions.

Purpose

This standard applies to all employees, contractors and third-party vendors with access to the State of Oklahoma's systems, networks and data.

Standard

- 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.

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

Effective date: 05/13/2024	**Review cycle:** Annual
Last revised: 05/13/2024	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	