OKLAHOMA
Office of Management
& Enterprise Services

Insider Threat Standard

Introduction

Insider threats pose a significant risk to the State of Oklahoma, but some steps can be taken to mitigate this risk. Establishing and adhering to a comprehensive Insider Threat Program (ITP) is crucial to effectively address this threat.

Purpose

This standard applies to all employees, contractors, and third-party vendors who have access to the organization's systems, networks and data.

Definitions

Insider threat – Any person with authorized access to an organization's systems, data or facilities who risks the confidentiality, integrity or availability of the organization's assets.

Insider Threat Program (ITP) – A structured set of policies, procedures and technologies designed to identify, manage and mitigate insider threats.

Standard

- Access Controls.
  - Cyber Command must establish strict access controls that limit user permissions based on their job responsibilities and work requirements. Access should be granted on a need-to-know basis and should be reviewed and updated regularly.
- Monitoring.
  - Cyber Command must establish monitoring procedures to detect any abnormal behavior or attempts to access unauthorized information. Cybercommand must employ technical and behavioral monitoring tools to detect abnormal activities. Monitoring should be conducted in a manner that is consistent with applicable laws, State of Oklahoma policies, procedures and regulations and should respect employee privacy.
- Background checks.
  - The ITP should require thorough background checks before hiring new employees to ensure they have no history of malicious activity or other red flags. Ongoing background checks should also be conducted for employees with access to sensitive information.
- Education and awareness.
  - Cyber Command must include education and awareness programs for employees to cover the various types of insider threats and provide guidance on how to identify and report suspicious activity. The programs should be regularly updated to reflect changes in the threat landscape.
- Audits and reviews.
  - Cyber Command must establish procedures for regular audits and reviews to identify potential vulnerabilities and ensure continued compliance with security protocols.

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

- Background Check Standard.
- Identity Management Standard.
- Simulated Phishing Standard.
- Security Awareness Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 11/01/2023	**Review cycle:** Annual
Last revised: 11/01/2023	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	