

Security Incident Response Standard

Introduction

The State of Oklahoma handles security incidents to minimize the impact on the confidentiality, integrity and availability of the state's systems, applications and data. It is especially important that security incidents are promptly communicated to Oklahoma Cyber Command to ensure all appropriate parties are involved early to assist with investigations, communications and reporting.

Purpose

This document establishes the requirements for reporting a security incident.

Definitions

- Data breach – The unauthorized access by an unauthorized person that results in access, use, disclosure or theft of non-public data or personal data.
- Non-public data – Data, other than personal data, not subject to distribution to the public as public information. Data is deemed sensitive and confidential by the State of Oklahoma when it contains information exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-public data includes any data deemed confidential by the State of Oklahoma as non-public data, or that a reasonable person would deem confidential.
- Personal data – Data containing 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) contains electronic protected health information that is subject to the Health Insurance Portability and Accountability Act of 1996, as amended.
- Security incident – The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with confidentiality, integrity and availability of state infrastructure.

Standard

Oklahoma Cyber Command utilizes the National Incident Management System (NIMS) framework for incident responses. NIMS integrates effective practices in emergency response into a comprehensive national framework for incident management.

All state agencies must report all security incidents and potential security incidents to Oklahoma Cyber Command immediately upon discovery. When an incident occurs, it is the responsibility of the agency to notify Oklahoma Cyber Command via email at cybercommand@omes.ok.gov.

All reported incidents are investigated, and prompt and full cooperation is required of agencies and all agency personnel.

As appropriate, Oklahoma Cyber Command acts as a liaison with law enforcement, risk management, legal counsel, agency leadership and state leadership.

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: 03/20/2026	Review cycle: Annual
Last revised: 03/20/2026	Last reviewed: 03/20/2026
Approved by: Dan Cronin, Chief Information Officer	