OKLAHOMA
Office of Management
& Enterprise Services

Security Exception Standard

Introduction

This standard outlines the requirements and procedure for requesting, evaluating and approving cybersecurity exceptions within the State of Oklahoma to ensure any deviations from established cybersecurity policies are justified, documented and managed in a way that minimizes risk.

Purpose

This standard applies to all employees, contractors and third-party vendors who operate on, or have access to, the State of Oklahoma information systems and assets.

Definitions

- Cybersecurity exception – A formal request to deviate from established cybersecurity policies, standards or controls.
- Risk assessment – The process of identifying, evaluating and prioritizing risks associated with a cybersecurity exception.
- Risk mitigation – Measures taken to reduce the risk associated with the security exception.
- Compensating controls – Measures or systems implemented to reduce or control risk.

Standard

Exceptions to standards are not ideal, however there are times when they may be necessary. Any request for an exception should be submitted to Cyber Command through a service desk support case. All requests must include:

- Documentation of the associated risks and a valid business justification.
- A detailed justification that specifies the policy or standard from which the exception is being requested.
- An outline of any compensating controls that will be implemented.

Cyber Command will conduct a formal risk assessment to determine potential risks. The State Chief Information Security Officer must review and approve all exception requests, with final approval from the State Chief Information Officer.

If approved, all exceptions are subject to ongoing review to assess compliance with conditions and ensure mitigation measures remain effective.

- Temporary exceptions will have a defined review period, typically 6–12 months.
- Exception renewal requires re-submission for approval with updated risk assessments.
- Exceptions will be terminated if the exception is no longer necessary or if compliance with the original standard becomes achievable.

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: 11/07/2024	**Review cycle:** Annual
Last revised: 11/07/2024	**Last reviewed:** 11/07/2024
Approved by: Aleta Seaman, Interim Chief Information Officer	