Information Technology Executive Council

ITEC 7052-P

1.0 TITLE: Information Security Exception Policy

2.0 PURPOSE: To establish a clear and structured process for requesting, evaluating, and approving security exceptions. Security exceptions are deviations from established security policies, standards, or controls, and this policy ensures that such deviations are carefully considered and appropriately mitigated.

3.0 SCOPE: The scope of this policy includes information, information systems and IT assets owned, managed, licensed, or leased by Entities.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas Executive branches, boards, commissions, departments, divisions, Entities, and third parties involved in processing, transmitting, or providing business capabilities on behalf of Kansas state government, hereafter referred to as Entities.

5.0 REFERENCES:

5.1 National Institute for Standards and Technology (NIST) Cyber Security Framework (CSF) 2.0

5.2 NIST Special Publication 800-53 Revision 5

6.0 DEFINITIONS:

6.1 Security Exception (Exception): A formal authorization to deviate from established security policies, standards, procedures, or controls for a defined period, with compensating controls in place to reduce risk.

6.2 Compensating Control: Alternative measures implemented to mitigate risks when the primary security control cannot be followed.

6.3 Risk Owner: The individual responsible for the business area impacted by the risk associated with the exception.

6.4 Approval Authority: Individuals with the authority to approve or deny security exception requests.

7.0 POLICY:

This policy is the principal governing authority for handling Information Security Exceptions by all Entities. While individual Entities retain the right to impose supplemental restrictions through their Entities-specific policies, such policies must not contradict the provisions outlined in this policy.

7.1 A Security Exception may only be granted by the Executive Branch Chief Information Security Officer, or their designee, for non-compliance with any security policy, standard, or requirement resulting from:

7.1.1 Impending retirement of a system.

7.1.2 Inability to implement the policy, standard, or control due to a limitation (e.g., technical constraint, business limitation or statutory requirement).

7.1.3 Implementation of a solution with equivalent protection to the requirements in the policy or standard.

7.1.4 Implementation of a solution with superior protection to the requirements in the policy or standard.

7.2 Security exceptions may be granted for a maximum of one year, after which an extension can be requested if still needed. An extension request must include a mandatory risk reassessment and justification for the continued need for the exception.

7.3 Security Exception requests must be completed using the KISO Exception Request Form signed by the following, as applicable per the policy and based upon the roles within the Entity:

7.3.1 Data or Information System Owner

7.3.2 Chief Information Officer

7.3.3 Entity Head

7.4 Signed KISO Exception Request Forms must be submitted to the Entity's Information Security Officer (ISO). The ISO is responsible for contacting the requesters to confirm receipt or request additional information, if needed.

7.5 Once all required information has been received, the CISO will review the submitted materials and either grant or deny the request.

7.5.1 Approved KISO Exception Requests will be returned to the requestor by the CISO.

7.5.2 Denied KISO Exception Requests will be returned with a brief explanation of why the request was denied.

7.5.3 If the agency does not agree with the KISO determination, the Entity must document that they will assume the risk of going forward, with written approval from the Entity head.

7.6 All security exceptions must be documented in a central repository managed by the Executive Branch CISO. This repository will be used to track exceptions, ensure periodic reviews, and facilitate audits. The repository must include details such as the nature of the exception, the risk assessment, compensating controls, and the review date.

8.0 RESPONSIBILITIES:

8.1 Heads of entities are responsible for establishing procedures for their organization's compliance with the requirements of this policy.

8.2 The Chief Information Security Officer, Executive Branch, is responsible for the maintenance of this policy.

9.0 CANCELLATION: Previous versions of this policy.