Information Technology Executive Council

ITEC 7044-P

1.0 TITLE: Information Security Risk Management Policy

2.0 PURPOSE: This policy establishes requirements for identifying, assessing, treating, and monitoring information security risks to Entity operations, information systems, and information.

3.0 SCOPE: The scope of this policy encompasses the processes, procedures, and activities related to identifying, assessing, treating, and monitoring information security risks to all data and information systems managed, processed, stored, or transmitted by Entities. This includes electronic, physical, and network-transmitted data, with an emphasis on addressing emerging threats, vulnerabilities, and compliance with evolving regulatory requirements. The policy applies throughout the entire risk management lifecycle, ensuring a consistent approach to protecting the confidentiality, integrity, and availability of all information assets.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas 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 Federal Information Processing Standards (FIPS) Publication 199

5.2 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0

5.3 NIST Special Publication (SP) 800-53 Revision 5

6.0 DEFINITIONS:

6.1 Information System: A combination of IT assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information or data.

6.2 Residual Risk: The portion of risk remaining after controls or countermeasures are applied.

6.3 Risk: The effect of uncertainty on objectives, which can have both positive and negative outcomes.

6.4 Risk Register: A central record of current risks and related information for a given scope or Entity, comprising both accepted risks and risks with a planned mitigation path.

6.5 Risk Tolerance: The level of risk or degree of uncertainty acceptable to an Entity, including examples such as system downtime, patching timeframes for vulnerabilities, and incident reporting timeframes.

6.6 Risk Treatment: The process used to modify risk.

7.0 POLICY: This policy serves as the principal governing authority for information security risk management by all Entities. While individual Entities may impose supplemental restrictions through their specific policies, such policies must not contradict the provisions outlined herein.

Entities must:

Security Categorization

7.1 Categorize all Information Systems according to FIPS Publication 199.

7.2 Ensure security categorization decisions receive approval from an Authorizing Official or designee.

Risk Assessment

7.3 Conduct information security risk assessments that:

7.3.1 Identify threats and vulnerabilities to the confidentiality, integrity, and availability of information and Information Systems.

7.3.2 Determine the impact and likelihood of harm from events leading to unauthorized access, use, disclosure, disruption, modification, or destruction of the Information System, and the information the Entity processes, stores, or transmits.

7.3.3 Identify controls in place to reduce the likelihood and impact of threats.

7.3.4 Include recommendations to reduce Residual Risk that exceeds the Entity's established Risk Tolerance.

7.3.5 Risk Treatment options are limited to:

7.3.5.1 Mitigate: Implement controls and safeguards to reduce risk to an acceptable level.

7.3.5.2 Transfer: Offset risk by outsourcing to a third party.

7.3.5.3 Accept: Formally accept low-level risks that do not significantly impact the organization.

7.3.5.4 Avoid: Cease activities or functions that pose significant, unmanageable risks.

7.4 Incorporate results and risk management decisions from mission or business process perspectives with Information System-level risk assessments.

7.5 Document risk assessment results in a formal risk assessment report and provide them to Entity leadership and Information System Owners.

7.6 Disseminate risk assessment results to authorized personnel on a need-to-know basis.

7.7 Review and update information security risk assessments until system decommissioning:

7.7.1 At least once every three (3) years.

7.7.2 Prior to operational implementation and after significant Information System changes.

7.7.3 When conditions arise that impact the security state of the Information System.

Risk Acceptance Criteria

7.8 Formally accept risks that cannot be fully mitigated but are determined to fall within an acceptable level of risk tolerance.

7.9 Ensure risk acceptance decisions are documented and authorized by a designated senior executive, such as the Chief Information Security Officer (CISO) or an equivalent senior official.

7.10 Ensure the following criteria must be met before acceptance:

7.10.1 The risk assessment must clearly outline the nature, impact, and likelihood of the risk.

7.10.2 All reasonably possible mitigation options must be documented and evaluated, and Residual Risks must be identified.

7.10.3 A formal risk acceptance statement must be signed by the designated senior official, acknowledging the potential impact and justification for accepting the risk.

7.10.4 Risk acceptance decisions must be reviewed periodically, at least annually, or whenever there is a significant change in the threat landscape, business environment, or Information System in question.

Incident Response and Risk Treatment

7.11 Incorporate any new risks identified during incident response activities into the risk management process.

7.12 Ensure when an incident occurs, risk treatment actions must be initiated to assess, document, and address newly identified vulnerabilities or risks. This process includes:

7.12.1 Conducting a post-incident risk assessment to identify vulnerabilities, threats, and weaknesses exposed during the incident.

7.12.2 Developing and implementing risk treatment plans that mitigate or eliminate newly identified risks.

7.12.3 Updating the Risk Register to reflect changes in the risk landscape and any Residual Risks following risk treatment efforts.

Documentation and Retention

7.13 Maintain comprehensive records of all risk assessments, risk treatment decisions, and risk acceptance statements. Documentation must include:

7.13.1 Formal risk assessment reports, including identified risks, assessed impact and likelihood, recommended treatments, and Residual Risks.

7.13.2 Risk treatment plans and the status of mitigation efforts.

7.13.3 Risk acceptance statements signed by the designated senior official.

7.14 Ensure records must be retained in accordance with applicable federal, state, and organizational record retention policies and laws.

7.15 The Entity's Information Security Officer is responsible for ensuring proper documentation.

Risk Register

7.16 Document and track all risk management decisions within a central Risk Register managed by the Entity's Information Security Officer.

7.17 Review, update, and report the status of risk response activities to Entity leadership semiannually or more frequently, as needed.

Continuous Improvement

7.18 Continuously improve their risk management processes to adapt to evolving threats and changing business needs. This includes:

7.18.1 Integrating lessons learned from security incidents, audits, and assessments to enhance the effectiveness of the risk management program.

7.18.2 Conducting periodic reviews and updates of risk management policies, procedures, and controls.

8.0 RESPONSIBILITIES:

8.1 Heads of Entities must establish procedures to ensure compliance with this policy.

8.2 The Chief Information Security Officer (CISO), Executive Branch, is responsible for maintaining this policy.

9.0 ENFORCEMENT:

9.1 Non-compliance with this policy may result in disciplinary action, including termination of employment for severe violations.

9.2 Written approval from the Kansas Information Security Office (KISO) is required for any exception to this policy.

10.0 CANCELLATION: This policy cancels and supersedes all previous versions.