Information Technology Executive Council

ITEC 7042-P

1.0 TITLE: Information Security Program Policy

2.0 PURPOSE: This policy defines and establishes roles and responsibilities for managing information security within the Entity. By clearly delineating responsibilities, the Entity ensures effective implementation and maintenance of its information security program in compliance with relevant standards.

3.0 SCOPE: This policy applies to all forms of data and systems, regardless of whether they are hosted internally, externally, or within cloud environments. It encompasses data, applications, networks, and other IT assets or services managed or operated by the State or any of its authorized agents.

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 K.S.A. 75-7236

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 Security Program Plan: A formal document providing an overview of the security requirements for an Entity-wide information security program, describing program management controls and common controls in place or planned for meeting those requirements.

6.2 Information System Component: A discrete identifiable IT Asset that represents a building block of an information system.

6.3 Plans of Action and Milestones (POA&M): A document identifying tasks to be accomplished, detailing required resources, milestones for meeting tasks, and scheduled completion dates.

7.0 POLICY: This policy is the primary governing authority for information security governance for all Entities. Individual Entities may impose supplemental restrictions via Entity-specific policies, provided they do not contradict this policy.

Entities must:

Information Security Program Plan

7.1 Develop and disseminate to authorized individuals an Information Security Program Plan that:

7.1.1 Describes the Entity's mission and critical business processes.

7.1.2 Provides an overview of security program requirements and describes program management controls and common controls in place or planned.

7.1.3 Describes the Entity's Information System Components.

7.1.4 Describes specific threats to the system that are of concern to the Entity.

7.1.5 Identifies and assigns roles, responsibilities, management commitment, and compliance obligations.

7.1.6 Reflects coordination among entities responsible for information security.

7.1.7 Receives approval from a senior official responsible and accountable for risk to Entity operations (including mission, functions, image, and reputation), assets, individuals, and other Entities.

7.2 Review and update the plan annually and following significant security events, audit findings, or changes to state and federal information security requirements.

7.3 Protect the plan from unauthorized disclosure and modification.

Information Security Roles and Responsibilities

7.4 Assign information security roles and responsibilities that:

7.4.1 Designate personnel to fulfill specific roles and responsibilities as identified in this policy.

7.4.2 Designated individuals must possess the necessary skills and expertise to manage and safeguard the Entity's information systems and data, ensuring the integrity of the Information Security Program.

7.4.3 Document designations formally, review annually, and update as needed to ensure clear and accountable implementation of information security.

7.5 Information Security Officer (ISO)

7.5.1 Ensure the ISO is responsible for leading the Entity's information security assurance efforts, which include:

7.5.1.1 Developing and maintaining local Entity information security policies and standards.

7.5.1.2 Identifying and recommending security requirements to limit information risks associated with the Entity's mission and business goals and objectives.

7.5.1.3 Leading, coordinating, and monitoring risk and security assessment activities.

7.5.1.4 Supporting third-party risk management by reviewing agreements, assessing vendors, applications, and services, and recommending risk treatment plans.

7.5.1.5 Liaising with internal and external auditors to manage controls for compliance with federal, state, and contract requirements.

7.6 Chief Information Officer (CIO) or the functional equivalent

7.6.1 Ensure the CIO oversees the Entity's information technology strategy and ensures that IT resources and infrastructure align with the Entity's mission and regulatory and security requirements, including:

7.6.1.1 Operating and supporting IT systems in compliance with approved security procedures, including IT asset management, malware protection, patch management, and data encryption.

7.6.1.2 Designing, acquiring, implementing, and operating systems in compliance with approved policies and standards.

7.6.1.3 Managing third-party IT service providers.

7.6.1.4 Monitoring the Entity's IT environment to identify, contain, and eliminate unauthorized activities as needed.

7.7 Information Owner

7.7.1 Ensure the Information Owner holds statutory or operational authority over specified information and establishes controls for its generation, collection, processing, dissemination, and disposal. Responsibilities include:

7.7.1.1 Assigning security categorization and protection standards and establishing appropriate use rules.

7.7.1.2 Ensuring compliance with applicable laws, regulations, contractual requirements, and policies for information collection and handling.

7.7.1.3 Providing input to Information System Owners regarding security requirements and controls for relevant systems.

7.8 Information System Owner

7.8.1 Ensure the Information System Owner oversees the procurement, development, integration, modification, or operation and maintenance of an information system, ensuring:

7.8.1.1 Security categorization and criticality are appropriately assigned.

7.8.1.2 The Information System operates in accordance with the System Security Plan and applicable requirements.

7.8.1.3 Sensitive information access is limited to those with a legitimate "need to know" or "need to use";

7.8.1.4 Security considerations are communicated to the Information Owner throughout the system's lifecycle.

Plans of Action and Milestones

7.9 Develop and maintain plans of action and milestones to address remedial information security and supply chain risk management actions.

7.10 POA&Ms must document necessary actions to respond to risks.

7.11 POA&Ms must be reported to Entity management at least quarterly or more frequently based on priority and severity.

7.12 Review POA&Ms for consistency and alignment with the Entity risk management strategy and priorities for risk response actions.

Risk Management Strategy

7.13 Establish and document their risk management strategy, defining risk appetite and tolerance, acceptable risk levels, and risk communication/reporting practices.

Mission and Business Process Definition

7.14 Define and document their mission and business processes, considering information security implications and resulting risks.

7.15 Determine and document information protection and processing needs resulting from the Entity mission and business processes.

7.16 Review and revise processes annually or as needed based on significant changes.

Continuous Monitoring Strategy

7.17 Implement a continuous monitoring strategy to:

7.17.1 Assess compliance with information security requirements.

7.17.2 Assign monitoring responsibilities.

7.17.3 Determine monitoring frequency and reporting metrics.

7.17.4 Periodically report on identified metrics.

Separation of Duties

7.18 Separate duties to minimize security risks for roles and operations that could impact Entity information assets.

7.19 Ensure individuals in governance, compliance, and auditing roles are independent of the functions they audit or assess.

7.20 Restrict access for roles like application developers, system administrators, and database administrators to maintain security.

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.