Information Technology Executive Council

Policy 7054-P

1.0 TITLE: Open-Source Software Security Policy

2.0 PURPOSE: The purpose of this policy is to establish a consistent and organized approach for evaluating, approving, implementing, monitoring, and retiring Open-Source Software (OSS) to ensure that its use supports the agency's mission while safeguarding the confidentiality, integrity, availability, and ownership of the State's information systems, software assets, and intellectual property.

3.0 SCOPE: This policy applies to all OSS used, embedded, or deployed by the Entity within systems that are categorized as Restricted-Use Information Systems or External Facing. This includes OSS integrated into applications developed in-house, incorporated through third-party development efforts, or acquired for direct use on agency-managed infrastructure or end-user devices.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas Executive Branch, 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) Cybersecurity Framework (CSF) 2.0

5.2 NIST Special Publication 800-53 R5

5.3 ITEC 7022-P Configuration Management Policy.

5.4 ITEC 1100-S Attachment A

6.0 DEFINITIONS:

6.1 Open-Source Software: Computer software that is released under a license that allows users to use, inspect, modify, enhance, or redistribute the source code.

6.2 Organizational User(s): As defined in ITEC 7038-P Personnel Security Policy

7.0 POLICY:

This policy is the principal governing authority for OSS use 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 Open-Source Software components used in infrastructure (e.g., Linux, Apache) must:

7.1.1 Be from a well-supported project with a public development history and frequent updates.

7.1.2 Be vetted for known vulnerabilities via trusted vulnerability databases (e.g., NVD, CISA KEV).

7.1.3 Be hardened in accordance with ITEC 7022-P Configuration Management Policy.

7.2 Embedded OSS libraries/frameworks for indirect use (e.g., development projects) must:

7.2.1 Be evaluated for license compatibility and intellectual property implications.

7.2.2 Be scanned for vulnerabilities.

7.2.3 Be from active projects with recent commits, defined maintainers, and robust issue tracking.

7.2.4 Be documented within an OSS Management Plan per ITEC 1100-S Attachment A.

7.2.5 Perform specific reviews or assessments against OSS that may exist within the product.

7.3 Entities are to develop internal procedures that address use of OSS on end-user devices, which must include guidance on the following topics:

7.3.1 Pre-approval and documentation of OSS use in the agency's software inventory.

7.3.2 Review of OSS licenses, end-of-life (EOL) conditions, and compliance with data security and system integrity requirements.

7.3.3 Assessment of risks related to data handling, export controls, and access control policies.

7.3.4 Validation of the authenticity of the software’s origin and update channels.

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