Information Technology Executive Council

ITEC 7022-P

1.0 TITLE: Configuration Management Policy

2.0 PURPOSE: This policy establishes standards to ensure baseline Configuration Settings are maintained to protect the confidentiality, integrity, and availability of State information assets.

3.0 SCOPE: This policy applies to all hardware, software, and associated infrastructure, such as network devices, security appliances, and cloud-based resources. It also covers third-party services integrated into the Entity's external presence, whether managed directly or indirectly.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas 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 Center for Internet Security (CIS) Benchmarks, as amended

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

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

5.4 NIST SP 800-70, as amended

5.5 NIST SP 800-128 Revision 3, as amended

6.0 DEFINITIONS:

6.1 Baseline Configuration: A set of specifications for a system or IT Asset within a system that has been formally reviewed and agreed upon. It serves as the basis for future builds, releases, and changes and can only be altered through change control procedures.

6.2 Configuration Management Plan: A comprehensive description of the roles, responsibilities, and governance documents (e.g., policies, standards, guidelines, and procedures) for managing the configuration of products and systems.

6.3 Configuration Settings: Parameters in hardware, software, or firmware that affect the security posture and functionality of an information system.

6.4 Information Systems or System: Combinations of IT assets used for collecting, processing, maintaining, sharing, disseminating, or disposing of information or data.

6.5 IT Asset: As defined in IT Asset Management Policy.

7.0 POLICY: This policy governs security-focused configuration management for all Entities. Entities may impose supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

Baseline Configurations

7.1 Develop, document, and maintain Baseline Configurations for Information Systems.

7.2 Review and update Baseline Configurations at least annually or when significant changes occur.

7.3 Use automated tools, such as Security Content Automation Protocol (SCAP) or CIS Configuration Assessment Tool (CAT), to maintain currency, completeness, accuracy, and availability of baseline configurations.

7.4 Retain at least one (1) previous version of the Baseline Configuration to support rollback.

7.5 Include the Information Security Officer or their designee as a member of the Entity's change control board or similar group.

Security Impact Analysis

7.6 Analyze system changes to determine potential security and privacy impacts before implementation.

7.7 Conduct post-implementation testing to verify that controls impacted by changes operate as intended and meet security and privacy requirements.

Access Restrictions for Change

7.8 Define, document, approve, and enforce physical and logical access restrictions for changes to hardware, software, and firmware components.

Configuration Settings

7.9 Configure IT Assets securely and consistently in accordance with CIS benchmarks, NIST-recommended configurations, or U.S. government configuration baselines.

7.10 Identify, document, and authorize deviations from mandatory security Configuration Settings.

7.11 Monitor and control changes to the Configuration Settings in accordance with this policy.

7.12 Install and maintain security tools provided by the Kansas Information Security Office (KISO) on all applicable IT Assets.

7.12.1 Each Regent's institution must install and maintain security tools provided by the respective Information Security Office, rather than the KISO.

7.13 Password-protect the BIOS, UEFI, or equivalent to prevent unauthorized access to low-level settings during boot.

Least Functionality

7.14 Configure systems according to the principle of least functionality, providing only mission-essential capabilities.

7.15 Prohibit or restrict ports, protocols, software, and services that are not required for business functions.

7.16 Limit component functionality to a single function per device. (e.g., email servers or web servers, but not both).

7.17 Disable insecure, unused, or unnecessary physical and logical ports/protocols to prevent unauthorized connections or data transfers.

7.18 Employ mechanisms to ensure only authorized software is executed and deny unauthorized programs.

Configuration Management

7.19 Develop, document, and implement Configuration Management Plans for Information Systems that:

7.19.1 Address roles, responsibilities, and configuration management processes.

7.19.2 Establish processes for identifying configuration items throughout the system lifecycle.

7.19.3 Define and manage configuration items for the system.

7.19.4 Are reviewed and approved by delegated management.

7.19.5 Protect the Configuration Management Plan from unauthorized disclosure and modification.

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.