Information Technology Executive Council

ITEC 7038-P

1.0 TITLE: Personnel Security Policy

2.0 PURPOSE: The purpose of this policy is to ensure that Executive Branch personnel have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner.

3.0 SCOPE: This policy applies to all Organizational Users, contractors, and third-party service providers involved in managing or accessing Information Systems on behalf of the State of Kansas. It ensures that personnel security standards are followed at all levels of the organization.

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. 75-3707e

5.2 K.S.A. 75-7240(b)(2)

5.3 K.S.A. 75-7241

5.4 K.S.A. 75-2949(f)

5.5 NIST CSF 2.0

5.6 NIST SP 800-53 R5

6.0 DEFINITIONS:

6.1 Access Agreements: Include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

6.2 Information Systems: As defined in the ITEC Configuration Management Policy.

6.3 Organizational Users: As defined in the ITEC Security and Privacy Awareness Training Policy.

7.0 POLICY: This policy governs personnel security standards for all Entities. While Entities may establish supplemental restrictions through their specific policies, these must not contradict the provisions outlined in this policy.

Entities must:

Personnel Screen

7.1 Screen Organizational Users before granting initial access to Information Systems.

7.2 Rescreen Organizational Users when rescreening is required.

Personnel Termination

7.3 Upon termination of Organizational User employment:

7.3.1 Disable login credentials on the same day the Organizational User ends employment.

7.3.2 Terminate or revoke all authenticators and credentials associated with the individual.

7.3.3 Retrieve from the terminated individual all IT Assets, security-related property, including authentication tokens, system manuals, keys, passwords, and identification cards.

Personnel Transfers

7.4 Review and confirm the need for current logical and physical access authorizations when individuals are reassigned or transferred within the Entity.

7.5 Modify access authorizations as needed to correspond with the reassignment or transfer.

7.6 Notify personnel responsible for logical and physical access administration no less than five (5) business days before the Organizational User's transfer.

Access Agreements

7.7 Develop and document an Access Agreement for the Entity

7.8 Review and update the Entity Access Agreement annually.

7.9 Require Organizational Users to acknowledge they have read, understand and agree to abide by the expectations set forth by the Access Agreement, before being granted access to Entity’s internal network.

7.10 Require re-signing of Access Agreements when updates are made or at least annually to maintain access.

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.