Information Technology Executive Council

ITEC 7046-P

1.0 **TITLE**: Security Awareness Training Policy

2.0 **PURPOSE:** The purpose of this policy is to ensure Organizational Users are aware of Information Security threats to the State's information assets, understand their responsibilities, and are aware of the statutory and policy requirements that are intended to protect State information and information systems from a loss of confidentiality, integrity, or availability.

3.0 **SCOPE:** This policy applies to all Organizational Users, contractors, and third-party service providers who access or manage IT Assets on behalf of the State of Kansas.

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. 75-7238(b)(8)

5.2 NIST CSF 2.0

5.3 NIST SP 800-53 R5

6.0 **DEFINITIONS:**

6.1 Organizational Users or Users: An employee or individual with similar status, such as interns, contractors, volunteers, or individuals from another Entity.

6.2 Telework (Telecommuting): As defined in the ITEC Telework Security Policy.

7.0 **POLICY:** This policy is the principal governing authority for security awareness training for all Entities. Entities may impose additional restrictions through Entity-specific policies, but these must not contradict this policy.

Entities must:

Information Security Awareness Training

7.1 Ensure Organizational Users complete introductory security awareness training within five (5) business days of the start date to their position and annually thereafter.

7.2 Ensure Organizational Users who do not complete their introductory or annual security awareness training within the established timeframes have their network accounts disabled until training is completed.

7.3 Ensue Organizational Users that transfer between Entities governed by this policy are compliant with mandatory annual security awareness training by demonstrating proof of completion within the current calendar year. This does not include or extend to agency specific regulatory compliance training.

7.4 Establish that Organizational Users on approved extended leave are exempt from completing security awareness training until such time as they return to work.

Training Content and Techniques

7.5 Require Organizational Users to complete introductory and/or annual security awareness training provided by the Executive Branch CISO. Entities may elect to provide replacement or additional security training upon prior written approval by the Executive Branch CISO.

7.6 Ensure contracts with vendors or suppliers that may access Restricted-Use Information (RUI) include language requiring the vendor to be trained appropriately.

7.7 Recognize security awareness techniques can include displaying posters, generating email advisories or notices, displaying logon screen messages, and conducting information security awareness events.

7.8 Revise security awareness training content annually or as changes in the risk environment change to ensure that it remains relevant.

7.9 Incorporate lessons learned from internal or external security incidents into training and awareness techniques.

Simulations

7.10 Conduct regular phishing simulations to assess Organizational Users' awareness and response to such threats.

7.10.1 The results of these simulations must be used to enhance training content and address identified weaknesses.

Role-Based Training

7.11 Provide role-based training for all Organizational Users that have unique or specific information security responsibilities.

7.12 Ensure training is completed by all telework users prior to beginning telework and annually thereafter. Fulltime telework personnel must complete telework training as part of their introductory security awareness training.

7.13 Update role-based training content annually to ensure relevancy.

7.14 Ensure that temporary workers, interns, and contract personnel receive security awareness training tailored to their role and access level.

Training Records

7.15 Document, update, and track completion of Organizational User's security awareness training activities, including all role-based training.

7.15.1 Entities that provide their own security awareness training must report security awareness training results and related details to the KISO or the entity CISO at least quarterly.

7.16 Retain all individual training records in accordance with records retention schedules.

Training Feedback and Effectiveness

7.17 Track the effectiveness of security awareness training programs through metrics such as completion rates, results of practical exercises, and post-training incident rates.

7.18 Ensure the Entity's Information Security Officer (ISO) reports on the security awareness training results and metrics to the Entity's senior management at least quarterly.

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.