Information Technology Executive Council (ITEC)

ITEC 7032-P

1.0 TITLE: Telework Security Policy

2.0 PURPOSE: This policy defines the security requirements and procedures for Organizational Users who telework to ensure the protection of the Entity's information and systems.

3.0 SCOPE: This policy applies to all Organizational Users authorized to telework and access the Entity's Information Systems, including remote access, use of personal devices, and any external connections to the Entity's networks and data. It covers all forms of data handling, system interactions, and security measures required during teleworking.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all boards, commissions, departments, divisions, and agencies of the State of Kansas, as well as any 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 of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5

6.0 DEFINITIONS:

6.1 Information Assets: A body of information managed as a single unit to be understood, shared, protected, and used effectively.

6.2 IT Assets: As defined in the IT Asset Management Policy.

6.3 Organizational User: An employee or individual with employee-like status, including contractors, volunteers, interns, or individuals detailed from another Entity.

6.4 Telework (telecommuting): A work arrangement where Organizational Users perform job duties from a location other than the traditional office, including home, satellite offices, coworking spaces, or other locations with internet access conducive to productivity.

7.0 POLICY:

This policy governs telework security for all Entities. Individual Entities may impose supplemental restrictions through their policies, provided these do not conflict with this policy.

Entities must:

Telework Security Training

7.1 Ensure authorized Telework users receive security training on:

7.1.1 Responsibilities outlined in this policy.

7.1.2 Potential risks to IT Assets, Information Assets, and interconnected State Entities.

7.1.3 Protection of authenticators, such as passwords, PINs, and hardware tokens.

7.1.4 Recognition and mitigation of social engineering attacks.

7.1.5 Consequences of disabling, altering, or circumventing security configurations.

7.1.6 Security incident management and breach disclosure procedures.

Telework User Responsibilities

7.2 Ensure authorized Telework users:

7.2.1 Adhere to all applicable security policies, standards, and procedures for using Entity Information Assets and IT Assets, regardless of location.

7.2.2 Do not connect personally owned devices to the State or Entity's IT infrastructure unless approved in advance by the CISO or an Entity authorized delegate.

7.2.2.1 Personally owned devices can be used on any State or Entity IT infrastructure that is a guest network or a public use network.

7.2.2.2 For all approved personally owned devices, each such device must comply with all State or Entity security configurations, including endpoint protection, encryption, and regular security updates, unless documented risk mitigation measures are in place.

7.2.3 Only connect to the State or Entity's IT infrastructure through Entity authorized encrypted virtual private networks (VPNs).

7.2.4 Physically secure IT Assets used to connect to the IT infrastructure.

7.2.5 Do not disable, alter, or circumvent established security controls, including endpoint protection software, host-based firewalls, and content filtering software.

7.2.6 Do not print sensitive documents in unsecured locations unless explicitly authorized and provided with secure printing solutions by the Entity.

7.2.7 Use only Entity-approved and managed devices for teleworking unless approved in advance by the CISO or authorized delegate.

7.2.8 Utilize only authorized software applications for conducting Entity business. The use of unauthorized or personal software applications is prohibited.

7.2.9 Acknowledge and understand that the Entity reserves the right to monitor telework activities, including access logs, usage patterns, and data transfers, to ensure compliance with this policy and applicable security requirements.

7.2.10 Log out of all Entity Information Systems when not actively in use and at the end of their teleworking session.

7.2.11 Immediately report any security incidents, suspected breaches, or loss of IT Assets to their Entity Information Security Officer (ISO).

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.