Information Technology Executive Council (ITEC)

ITEC 7012-P

1.0 TITLE: Remote Access Security Policy

2.0 PURPOSE: This policy establishes uniform security controls for remote access across all applicable Entities.

3.0 SCOPE: This policy applies to all remote access activities involving non-public State of Kansas networks, systems, applications, and services. It governs the use of remote access technologies, including Virtual Private Networks (VPNs), secure web gateways, and other methods used to connect to the State's internal networks from external locations.

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 Systems: As defined in ITEC Information Security Program Policy.

6.2 Multi-Factor Authentication (MFA): An authentication method requiring two or more different pieces of evidence to confirm a user's claimed identity, such as something the user knows, has, or is.

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

6.4 Remote Access: Access to State information by users or processes communicating through external networks, such as the Internet, to non-public Entity networks.

6.5 Virtual Private Network (VPN): A secure link that uses tunneling, security controls, and endpoint address translation, simulating a dedicated line.

7.0 POLICY:

This policy governs the security of remote access to all State of Kansas Entities. Entities may impose supplemental restrictions through their policies, provided these do not conflict with this policy.

Entities must:

Remote Access Control

7.1 Strictly control remote access to non-public State networks, systems, applications, and services.

7.2 Permit authorized Organizational Users to connect remotely to conduct State-related business only through secure, authenticated, and Entity-approved access methods, with prior Entity management approval based on business needs.

7.3 Do not automatically grant access to internal networks; access must be explicitly requested by the user and approved by the system manager.

7.4 Establish and document usage restrictions, configuration requirements, and implementation guidance for each type of remote access allowed.

Monitoring and Logging

7.5 Collect and maintain logs of all remote access sessions, including session details such as time, duration, user identity, and actions performed, to support auditing and compliance reviews.

7.6 Ensure remote access is treated as a privilege and deny access to Organizational Users that pose unacceptable security or privacy risks.

Authentication and Revocation

7.7 Require MFA for all remote access to Entity Information Systems.

7.8 Revoke remote access at any time for reasons including non-compliance with security policies, request by the user's supervisor, or adverse impact on network performance due to remote connections.

7.9 Terminate remote access privileges upon an employee’s or contractor’s termination and review access upon changes in assignment or during scheduled account reviews.

7.10 Prohibit anonymous remote logins (e.g., using “guest” accounts) except on publicly accessible systems where users are anonymous.

Tunneling and Connection Controls

7.11 Implement controls to prevent split tunneling for remote devices unless necessary for Entity business and securely provisioned.

7.12 Provide remote access through technologies and methods authorized by the Executive Branch Chief Information Technology Officer (CITO) or their designee(s). Regent institutions

may authorize additional methods in collaboration with CITO, provided these methods align with the security requirements, guidelines, and statewide security policies established by the Executive Branch.

7.13 Route all remote access sessions through State managed or Regent institution managed network access control points.

7.14 Implement FIPS 140-2 (or its successor) compliant encryption techniques to protect the confidentiality and integrity of remote access sessions.

Connection Criteria and Session Management

7.15 Configure remote access infrastructure to force an automatic disconnect after thirty (30) minutes of inactivity.

7.16 Configure VPN technologies to limit sessions to no more than twelve (12) consecutive hours before requiring a forced disconnect and reestablishment of the session.

7.17 Restrict remote network connections for vendors or third parties to only when needed for a valid business function and immediately deactivate access after use.

Device Security Validation

7.18 Validate the patch level and software versions of devices attempting to connect, where technically feasible.

7.19 Prevent connections until devices have the latest security patches installed, where technically feasible.

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.