Information Technology Executive Council

ITEC 7034-P

1.0 TITLE: Acceptable Use of IT Policy

2.0 PURPOSE: This policy establishes minimum requirements for the acceptable use of IT Resources to protect users' resources. Inappropriate use exposes the State network to risks such as ransomware, viruses, system compromises, data breaches, and legal liabilities. This policy does not cover every possible scenario and does not relieve anyone accessing an IT system from their obligation to exercise good judgment.

3.0 SCOPE: This policy applies to all Organizational Users, contractors, and third-party service providers who access, manage, or maintain IT Resources on behalf of the State of Kansas. It covers all activities related to the use, management, and security of IT Resources, including hardware, software, networks, and data.

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. 21-5611

5.2 K.S.A. 21-5839

5.3 K.S.A. 21-6002

5.4 NIST CSF 2.0

6.0 DEFINITIONS:

6.1 Information Resources: Information and related resources, such as the internet, personnel, equipment, funds, and IT Assets.

6.2 IT Assets: As defined in IT Asset Management Policy

6.3 Organizational Users (Users): As defined in Security and Privacy Awareness Training Policy.

6.4 System Owner: The individual or department responsible for the overall ownership, operation, and security of a particular IT system.

7.0 POLICY: This policy governs acceptable use of Information Resources for all Entities. Entities may impose supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

7.1 Ensure Organizational Users are individually responsible for appropriate use of IT Resources assigned to them.

7.2 Ensure IT Resources are provided for official business purposes. Organizational Users must only access IT Resources necessary for their assigned duties.

7.3 Ensure Organizational Users do not attempt to access or provide resources to access restricted portions of the network, operating systems, security software, or administrative applications without prior authorization from the System Owner or delegate.

7.4 Prohibit Organizational Users from using IT Resources for illegal or unlawful purposes, including but not limited to copyright infringement, personal gain, libel, slander, fraud, defamation, forgery, impersonation, and spreading malware.

7.5 Ensure Organizational Users maintain the security and confidentiality of information, safeguarding login credentials, and securing Restricted-Use Information per ITEC security policies. Unauthorized access, sharing, or disclosure of Restricted-Use Information is prohibited.

7.6 Inform Organizational Users that there is no expectation of privacy when using State-issued IT Resources. All usage, including emails, messaging, internet activity, and data storage, may be monitored to ensure policy compliance and security operations.

7.7 Ensure Organizational Users return all IT Assets and associated data upon separation from employment or contract termination.

7.8 Prohibit Organizational Users from using State-owned licensing keys on personal devices without approval from the CITO or delegate.

7.9 Prohibit Organizational Users from storing Entity Restricted-Use Information in unauthorized locations.

7.10 Ensure Organizational Users do not use personal devices to access IT Resources unless authorized in advance by the Executive Branch Chief Information Security Officer or designee. Regent's CISO or their equivalent may provide the approval for their specific agency.

7.11 Inform that violations of this policy by contractors or third-party service providers must result in termination of contracts and/or legal action.

7.12 Ensure Organizational Users immediately report any event that threatens the availability, integrity, or confidentiality of IT Resources or data, violates policies, or contravenes applicable laws, to the Kansas Information Security Office (KISO) or 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 Violations must be documented and reported to KISO.

9.3 Repeated or serious breaches may result in suspension of IT access or further legal action.

9.4 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.