Information Technology Executive Council (ITEC)

ITEC 7028-P

1.0 TITLE: Media Protection Policy

2.0 PURPOSE: This policy establishes requirements for protecting data in all forms and media throughout their lifecycle based on sensitivity, criticality, value, and the impact of a loss of confidentiality, integrity, and availability on applicable stakeholders.

3.0 SCOPE: This policy applies to all digital and non-digital media used to store, process, or transmit Restricted-Use Information (RUI).

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas branches, 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. 45-221

5.2 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, as amended

5.3 NIST Special Publication (SP) 800-53 Revision 5, as amended

5.4 NIST SP 800-88 Revision 1, as amended

6.0 DEFINITIONS:

6.1 Digital Media: Includes diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks.

6.2 Media: Collective term for Digital and Non-Digital Media.

6.3 Non-Digital Media: Includes paper and microfilm.

6.4 Organizational User: As defined in the Personnel Security Policy.

6.5 Restricted Use Information (RUI): As defined in ITEC Standard 7230a.

6.6 Sanitization: A process to remove information from media such that data recovery is not possible, including the removal of all labels, markings, and activity logs.

6.7 Telework: As defined in the Security Awareness Training Policy.

7.0 POLICY: This policy governs the safeguarding and sanitization of data, regardless of form or media, by all Entities. Entities may impose supplemental restrictions through their specific policies, but such policies must not contradict the provisions outlined here.

Entities must:

Clean Desk and Clear Screen

7.1 Protect digital and non-digital information from unauthorized access and disclosure.

7.1.1 Secure file cabinets or other appropriate containers when Restricted Use Information is left unattended.

7.1.2 Clear desks during non-working hours to prevent unauthorized access and disclosure of Restricted Use Information.

7.1.3 Ensure documents containing Restricted Use Information are not left unattended on printers, copiers, or fax machines.

7.1.4 Invoke screen-lock before leaving secured work areas.

7.1.5 Position displays or screens so they are not visible to unauthorized individuals. Use privacy filters on laptops and displays if working in shared or public spaces.

7.1.6 Ensure workspace backgrounds are free from visible Restricted Use Information during virtual meetings, video calls, or while working in a shared or public environment.

7.1.6.1 Ensure when the workspace background is not able to be clean and free from visible RUI, then Entity approved virtual backgrounds must be used.

7.1.7 Require Entity approved virtual backgrounds to be used during video calls to obscure and prevent the accidental disclosure of Restricted Use Information.

7.1.8 Ensure Telework setups are in a private or controlled space whenever possible to minimize the risk of unauthorized observation.

Media Access

7.2 Restrict access to authorized personnel for all records and information protected from open records disclosure, legal requirements, or prohibited by contract on Digital and Non-Digital Media.

Media Marking

7.3 Mark Media with appropriate classification labels, distribution limitations, and handling caveats.

7.3.1 Media containing only data that is classified as Public requires no marking or labels.

Media Storage

7.4 Securely store Media that contains Restricted Use Information within a controlled area with restricted access for authorized personnel.

7.4.1 Encrypt all Restricted Use Information that is stored on diskettes, magnetic tapes, external or removable hard disk drives, and flash drives.

7.4.2 Store Media that is not actively being used in locked drawers or cabinets within controlled areas.

7.5 Classify and label media to indicate the classification of the information.

Media Transport

7.6 Implement safeguards to ensure the confidentiality and integrity of Restricted Use Information contained on Media during transport outside of controlled areas.

7.7 Ensure accountability and restrict transport activities to authorized personnel or Entity approved services (i.e., United States Postal Service, etc.).

7.8 Inform Organizational Users of their responsibilities and provide them with necessary tools and training to protect Media and assets during transport.

Media Sanitization

7.9 Sanitize all Media according to current NIST SP 800-88 guidelines prior to disposal or reuse.

7.9.1 If Digital Media will be reused by the Entity for the same purpose of storing Restricted Use Information and will not be leaving Entity control, then clearing is a sufficient method of sanitization.

7.10 Require and maintain documentation of verification of sanitization and disposal actions (i.e., certificates of destruction, chain of custody logs, etc.).

Media Use

7.11 Restrict the use of Digital Media and related devices in Entity IT assets to only Entity approved devices, devices provided by the Entity, and devices not personally owned.

7.12 Prohibit the use of Digital Media and related devices in Entity IT assets when such devices have no identifiable owner.

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.