Information Technology Executive Council

ITEC 7040-P

1.0 TITLE: Physical and Environment Security Policy

2.0 PURPOSE: This policy establishes requirements to ensure that Entities' information assets are protected by physical controls to prevent tampering, damage, theft, or unauthorized physical access.

3.0 SCOPE: This policy applies to all Organizational Users, contractors, and third-party service providers who manage or access IT systems and facilities 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 NIST CSF 2.0

5.2 NIST SP 800-53 R5

6.0 DEFINITIONS:

6.1 Controlled Areas: Collective term for Operations and Restricted Access Zones.

6.2 Operations Zone: A general access area where Entity business activities or support services are regularly conducted.

6.3 Restricted Access Zone: An area that requires specific authorization granted by the owner of each restricted zone, including data centers, server rooms, cable cabinets, and communication equipment rooms.

7.0 POLICY: This policy governs physical and environmental security measures for protecting information and information systems. Entities may establish supplemental restrictions, but these must not contradict this policy.

Entities must:

Physical Access Authorizations

7.1 Develop, approve, and maintain a list of individuals authorized to access Controlled Areas. When hosting is outsourced, ensure vendors maintain similar lists for Restricted Access Zones.

7.2 Annually review and approve access lists to Controlled Areas.

7.3 Remove access (including from the access list, keys, badges, and combination changes) when it is no longer required or upon termination.

7.4 Develop and implement procedures for reporting and responding to physical security breaches or incidents, which must include immediate notification to the appropriate Entity incident response teams.

7.5 Implement procedures for issuing, tracking, and auditing physical access credentials, including keys and badges to Restricted Access Zones.

7.5.1 Lost or stolen credentials must be reported immediately, and replacement credentials must be issued only after verification of need.

Physical Access Controls

7.6 Enforce access authorizations at entry and exit points of Restricted Access Zones by:

7.6.1 Verifying individual access authorizations before granting access.

7.6.2 Controlling access, including ingress and egress, using physical access control systems, devices, or guards.

7.7 Maintain visitor logs for Restricted Access Zones.

7.8 Escort visitors and monitor their activity within Restricted Access Zones.

7.9 Secure unused IT assets by moving them to designated secure areas if not in use for extended periods.

7.10 Annually inventory keys used for securing Restricted-Use Information.

7.11 Combinations and/or keys must be changed when:

7.11.1 A key inventory reveals a missing or unaccounted-for key.

7.11.2 Combinations are compromised or suspected of being compromised.

7.12 Conduct physical security risk assessments at least annually to identify vulnerabilities and ensure the adequacy of physical controls.

7.12.1 Risk assessments must be documented, and any identified gaps must be addressed through remediation plans.

7.13 Ensure that third-party vendors and contractors comply with physical and environmental security requirements. Contracts with external providers must include provisions for physical security compliance.

7.14 Ensure that appropriate signage is placed at all entry points to Restricted Access Zones, informing personnel and visitors of access restrictions.

7.14.1 Signage must also indicate emergency procedures, such as the location of emergency exits and emergency shutoff controls.

Third-Party Risk Management

7.15 Ensure third-party data center hosting providers have implemented physical and environmental security requirements.

7.16 Ensure contracts with external providers must include provisions for physical and environmental security requirements.

Access Control for Output Devices

7.17 Control physical access to output from printers, scanners, fax machines, and copiers by placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only or placing output devices in locations that can be monitored by personnel to prevent unauthorized individuals from accessing output.

7.18 Control access to storage locations of output devices.

Monitoring Physical Access

7.19 Maintain physical access logs to data centers.

7.20 Review physical access logs monthly or upon the occurrence of a potential security event.

7.21 Monitor physical access to public access facilities where IT assets reside to detect and respond to physical security incidents.

7.22 Review physical access logs monthly or upon the occurrence of a potential security event.

7.23 Coordinate results of reviews with the Entity incident response team.

7.24 Audit physical and environmental controls, including access control systems, power systems, fire detection and suppression systems, and other environmental protections, at least annually to ensure they are functioning as intended.

7.24.1 Audit results must be documented, and any deficiencies must be promptly addressed.

7.24.2 Where hosting has been outsourced to a third-party hosting provider, Entities must conduct annual reviews of independent audit reports or conduct onsite reviews.

Incident Response

7.25 Conduct a post-incident review after any physical or environmental security incident to identify weaknesses in controls, improve security measures, and document lessons learned.

7.26 Post-incident review results must be shared with relevant stakeholders and Entity leadership.

Visitor Access Records

7.27 Maintain visitor access records for Controlled Areas in compliance with retention requirements. Records must include:

7.27.1 Name and organization of the visitor.

7.27.2 Visitor's signature.

7.27.3 Form of identification and initials of the verifying guard or person.

7.27.4 Date of access.

7.27.5 Time of entry and departure.

7.27.6 Purpose of visit.

7.27.7 Name of the person visited.

7.28 Review visitor access records monthly.

7.29 Report any anomalies in visitor access records to security personnel.

Power Equipment and Cabling

7.30 Protect power equipment and cabling from damage and destruction.

Emergency Shutoff

7.31 Ensure that data centers have the ability to shut off power in emergency situations.

7.32 Protect data center emergency shutoff systems from unauthorized activation.

Emergency Power

7.33 Ensure emergency power systems are implemented to provide continuous power and protect against power surges.

Emergency Lighting

7.34 Ensure data centers maintain automatic emergency lighting that activates during power outages and covers emergency exits and evacuation routes.

Fire Protection

7.35 Ensure data center fire detection and suppression systems are maintained and supported by independent power sources.

Environmental Controls

7.36 Maintain temperature and humidity controls within service level agreements (SLA) in data centers.

7.37 Monitor and alert facility management and IT personnel in the event of significant temperature changes in data centers

7.38 Ensure data centers are equipped with redundant humidity control, ventilation, and air conditioning (HVAC) systems to maintain optimal environmental conditions and support continuous operation.

Water Damage Protection

7.39 Protect data centers from water damage by providing master shutoff or isolation valves that are accessible, functional, and known to key personnel.

Location of IT Assets

7.40 Position IT assets within facilities to minimize damage from physical and environmental hazards and unauthorized access.

Asset Monitoring and Tracking

7.41 Implement asset location tracking technologies to monitor the location and movement of unattended IT assets.

Facility Location

7.42 Consider physical and environmental hazards when selecting locations for storing, processing, or transferring Restricted-Use Information and Mission Critical Information Systems.

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.