# Information Technology Executive Council

## ITEC 7036-P

**1.0 TITLE**: IT Hardware Maintenance Security Policy

**2.0 PURPOSE:** The purpose of this policy is to ensure IT Assets are properly maintained to minimize risks from emerging information security threats and prevent the potential loss of confidentiality, integrity, or availability due to system failures.

**3.0 SCOPE:** This policy applies to all Organizational Users, contractors, and third-party service providers who manage or maintain IT Assets on behalf of the State of Kansas. It covers all maintenance-related activities to ensure the proper function and security of IT Assets.

**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 SP 800-53 R5

5.2 NIST CSF 2.0

**6.0 DEFINITIONS:**

6.1 Field Maintenance: the type of maintenance conducted on an IT Hardware Asset after it has been deployed to a specific site (i.e., operational environment).

6.2 IT Hardware Assets: Hardware components that make up the IT infrastructure of an Entity.

6.3 Nonlocal Maintenance: Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.

**7.0 POLICY:** This policy governs maintenance activities for IT Assets by all Entities. Entities may implement supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

Controlled Maintenance

7.1 Schedule, document, and review records of maintenance, repair, and replacement on IT Hardware Assets according to manufacturer or vendor specifications and/or Entity requirements.

7.2 Approve and monitor all maintenance activities, whether performed on-site or remotely, and whether the IT Hardware Assets are serviced on-site or removed to another location.

7.3 Explicitly approve the removal of IT Hardware Assets from Entity facilities for off-site maintenance, repair, or replacement.

7.4 Sanitize IT Hardware Assets to remove Restricted-Use Information from associated media before removal from Entity facilities for off-site maintenance, repair, or replacement.

7.5 Verify that all potentially impacted controls are functioning properly following maintenance, repair, or replacement activities.

7.6 Include the following information in IT Hardware Asset maintenance records:

7.6.1 Date and time of maintenance.

7.6.2 Description of maintenance performed.

7.6.3 Names of individuals or groups performing maintenance.

7.6.4 Name of escort.

7.6.5 System components or equipment that is removed or replaced.

7.7 Ensure all maintenance activities must be logged and audited regularly to verify compliance with this policy.

7.8 Ensure maintenance logs must be reviewed periodically by designated personnel to identify unauthorized activities or inconsistencies.

7.9 Ensure maintenance activities must be coordinated with the Entity's risk management and/or change management processes to identify, assess, and mitigate potential risks to system integrity and security.

7.10 Establish communication protocols for reporting incidents or issues that arise during or following maintenance activities.

Maintenance Tools

7.11 Approve, control, and monitor the use of system maintenance tools.

7.12 Review previously approved system maintenance tools at least annually.

7.13 Inspect maintenance tools used by personnel for unauthorized modifications and ensure the latest software updates and patches are installed.

7.14 Check media containing diagnostic and test programs for malicious code before use in systems.

7.15 Prevent the removal of maintenance equipment containing Entity information by:

7.15.1 Verifying no Restricted-Use Information is contained on the equipment.

7.15.2 Sanitizing or destroying the equipment.

7.15.3 Retaining the equipment within the facility.

7.15.4 Obtaining a documented exemption from the Kansas Information Security Office (KISO) or Entity Information Security Officer (ISO), authorizing removal of the equipment.

Nonlocal Maintenance

7.16 Approve and monitor Nonlocal Maintenance and diagnostic activities.

7.17 Allow the use of Nonlocal Maintenance and diagnostic tools only when consistent with ITEC policy and documented in the system security plan.

7.18 Employ strong authentication for establishing Nonlocal Maintenance and diagnostic sessions.

7.18.1 Require strong authenticators resistant to replay attacks and employing multi-factor authentication, such as PKI certificates stored on a token protected by a password, passphrase, or biometric.

7.19 Maintain records for Nonlocal Maintenance and diagnostic activities.

7.20 Terminate sessions and network connections when Nonlocal Maintenance is completed.

Maintenance Personnel

7.21 Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance personnel or organizations.

7.22 Verify that non-escorted personnel performing maintenance possess required access authorizations.

7.23 Designate Entity personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel without the required authorizations.

Timely Maintenance

7.24 Obtain maintenance support and/or spare parts for Mission Critical Systems and system components consistent with Entity defined Recovery Time Objectives (RTOs).

Field Maintenance

7.25 Restrict or prohibit Field Maintenance on IT Hardware Assets that have been deployed to remote locations.

7.26 Maintain records for Field Maintenance and diagnostic activities.

**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.