Information Technology Executive Council

ITEC 7018-P

1.0 TITLE: IT Asset Management Policy

2.0 PURPOSE: This policy establishes a uniform approach to IT Asset management to ensure that components of the state network are accounted for and visible to software tools for monitoring the attack surface.

3.0 SCOPE: This policy applies to all IT assets owned, leased, or licensed by the Entity.

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 CIS Guide to Enterprise Assets and Software, as amended

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 1800-5, as amended

6.0 DEFINITIONS:

6.1 Application: A system for collecting, saving, processing, and presenting data by means of a computer. It can be executed as a component of software and is often synonymous with software application.

6.2 Application Programming Interface (API): A system access point or library function with a well-defined syntax, accessible from application programs or user code, providing specific functionality.

6.3 End-User Devices: Mobile and portable devices, such as laptops, smartphones, tablets, desktops, and workstations; a subset of IT Assets.

6.4 Industrial Control System (ICS): Encompasses control systems such as SCADA, DCS, and PLCs commonly found in industrial sectors and critical infrastructures.

6.5 Internet of Things (IoT): T A network of devices equipped with hardware, software, firmware, and actuators that connect, interact, and exchange data.

6.6 IT Asset: Information technology assets, including hardware, software, and firmware.

6.7 Software: Computer programs and associated data that may be dynamically written or modified during execution.

6.8 Utilities: Software that provides specific services to maintain, optimize, and enhance a computer system's functionality.

7.0 POLICY: This policy governs IT Asset Management for all State of Kansas Entities. Entities may impose supplemental restrictions through specific policies, but these must not contradict this policy.

Entities must:

7.1 Maintain an accurate, detailed, and up-to-date inventory of all State-owned, leased, licensed, or managed IT Assets.

7.2 Inventory IT Assets, including software (applications, source code, system software, development tools, and Utilities), equipment (end-user devices, physical and virtual servers, network devices), non-computing/IoT devices (ICS, printers, physical security sensors, magnetic and optical media), and services (locally hosted, cloud computing, communications services, service accounts, and APIs).

7.3 Ensure inventories have sufficient granularity for tracking and reporting.

7.4 Review and update inventories annually and as part of installation removals and system updates.

7.5 Utilize automated tools, when possible, to maintain the currency, completeness, accuracy, and availability of inventories.

7.6 Identify and address unauthorized IT Assets promptly by removing them from the network, denying remote connections, or quarantining the assets.

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.