Information Technology Executive Council (ITEC)
ITEC-1100-S

1.0 TITLE: Software Use and Licensing Standard

1.1 Effective Date: June 20, 2023

1.2 Type of Action: New

2.0 PURPOSE: To define the ITEC-1100-P minimum standards and procedures.

3.0 ORGANIZATIONS AFFECTED: All Branches, Boards, Commissions, Departments, Divisions, and Entities of state government, hereafter referred to as entities.

4.0 REFERENCES:

4.1 State of Kansas ITEC-7230-A – Enterprise Security Policy

4.2 State of Kansas ITEC-8010-P- Kansas Data Review Board Policy

4.3 Software End of Life Management Plan – Attachment A

4.4 Software Inventory Template – Attachment B

5.0 DEFINITIONS:

5.1 Authorized personnel - Any appropriately identified individual with a requirement to have elevated security access and or administrative rights to perform IT tasks that are outside normal user functions.

5.2 End-of-Life (EOL) – applies to both computer hardware and software, is the stage of a product in which it becomes outdated or unsupported by the manufacturer. An end-of-life announcement by a vendor stipulates when the manufacturing will end, or if already ended, how far into the future support for the product will be provided.

5.3 Information Asset Trustee – Per ITEC-7230a, entities must ensure that Information Asset Trustees are appointed for the following information assets:

5.3.1 Intellectual property or

5.3.2 Data compilations that contain or may be projected to contain source records on thirty (30) or more individuals of Restricted-Use Information.

5.4 License – The owner of a copyright owns the exclusive right to reproduce, modify (create “derivative works”), distribute, perform, and display the item in which the owner holds the copyright. Patent and trademark owners have similar rights. The owner of a copyright may authorize others to exercise these rights, usually through the granting of a license.

5.5 Ownership – Owning a copyrighted item does not give the possessor rights in the copyrighted work. Possession of a material object that embodies the copyrighted work does not of itself convey any rights in the actual copyright. Oftentimes, the copyright owner reserves all rights of ownership, and only provides specifically delineated usage rights through a license. Similar protections apply to patents and trademarks.

5.6 Open-Source Software (OSS) - Computer software that is released under a license that allows users to use, inspect, modify, enhance, or redistribute the source code.

6.0 PROCEDURES:

6.1 All entity-used software shall be protected against loss and unauthorized copying, installing, downloading, and accessing.

6.1.1 Access to software must be controlled using appropriate system permissions given to authorized personnel.

6.1.2 Storage media such as CDs, DVDs, USB drives, tape drives, or other media containing software must be stored securely within a controlled area and physical access to that controlled area must be restricted to authorized personnel.

6.1.3 Systems must be configured to restrict the installation, configuration, or removal of software to authorized personnel.

6.2 Software that is no longer required will be decommissioned and installations removed. Copies and packages will be archived or destroyed in compliance with the vendor's requirements. Support and maintenance shall be canceled, and contracts or subscriptions shall be terminated as appropriate. All entities' data must be removed from vendor systems and confirmation of removal obtained upon termination of services.

6.2.1 All entities should establish controls over vendor-hosted data before any agreement with a vendor is signed. Contracts must include clear information regarding entities' access and rights to data not only while hosted but during any transition, including the method for recovery, transfer, and deletion to comply with the policy.

6.2.2 Contracts or agreements with the vendor shall address the terms to recover data at termination. Entities must fully understand the vendors' architecture and processes as this is evolving for applications that are hosted in the cloud or have data in cloud environments. Entities should review the guidelines provided by the vendor and the cloud provider (if not the same).

6.3 End-of-life (EOL) licensing: entities shall ensure that software is properly licensed throughout the period of use. Refer to attachment A – Software End of Life Management Plan.

6.3.1 There are typically five steps in an application EOL, they are:

- EOL Planned (EOLP) Announcement
- End of Sales (EOS)
- End of Maintenance (EOM)
- End of Standard Support (EOSS)
- End of Life (EOL)

6.3.2 The entity should start identifying business and security risks related to the continuing use of the application after the vendor's "EOL Planned Announcement" step.

6.3.3 Entity shall create and implement a risk mitigation plan related to the application's EOL. Refer to Risk Analysis section in Attachment A Software End of Life Management Plan.

6.4 Software Inventory

6.4.1 A software inventory must be established by all entities to track the purchase of all software, license or end-user license agreements, documentation, and related items.

6.4.2 Entities must create and maintain a software inventory, update the inventory as changes occur, and review the inventory at least annually. Software inventory information must be preserved indefinitely. Refer to attachment B Software inventory Template.

6.4.3 Tracking of software inventory begins from time of order placement throughout the life of the item if ownership is retained.

6.4.4 The software inventory must include the following data. Entities may choose to expand upon the inventory data beyond what is listed below.

- Title of Software
- Type of Software License
- Description (i.e., software name)
- Version
- Publisher
- Software Serial/ Registration Number (if available)
- License period if applicable
- Purchase Order number or Unique Identifier (such as Voucher ID used in the SMART system)
- Date purchased
- Cost
- Number of Entitlements
- Location Compliance– verification that the physical location of software, servers, and data are within the United States.
- End of Life

6.4.4.1 Any externally managed system, such as Software as a Service, should be included in the entity's software inventory.

6.4.5 Each entity shall be responsible for updating the software inventory to identify unused software to make sure it is uninstalled, retired, or reassigned.

6.4.6 Each entity shall be responsible for updating the software inventory to identify applications that are End of Life. Applications that have reached End of Life status are to be uninstalled from the environment and then marked as no longer needed (NLR) or retired.

6.4.7 The entity Information Asset Trustee must approve the removal or retirement of software. Each entity is responsible for removing the software from the corresponding hosting environment. Disposal of software must comply with any software manufacturer or publisher agreements. All physical media and paperwork per agreements will be destroyed based on the entity's retention schedule.

6.5 Open-Source Software (OSS) Use and Licensing

6.5.1 Open-source software (OSS) is considered to be commercial software and must comply with laws, regulations, IT security, and other policies that apply to commercial software.

6.5.2 State entities are required to develop and maintain an Open-Source Software Management Plan. This plan should include an inventory of all OSS development, source code repository location, on-going support plan (including IT security and vulnerability management, disaster recovery and business continuity) and the business use case for each OSS with-in the entity's environment. Refer to Software End of Life Management Plan Attachment A, Open-Source Software section.

6.5.3 Prior to starting any development or procurement process involving OSS, per ITEC Policy 8010-P state entities should notify the Information Asset Trustee to document licensing terms and OSS Management Plan.

7.0 RESPONSIBILITIES:

7.1 Heads of entities are responsible for establishing procedures for their organization's compliance with the requirements of this policy.

7.2 The Chief Information Technology Officer, Executive Branch, is responsible for the maintenance of this policy.

8.0 CANCELLATION: No previous versions of this standard.

9.0 HISTORY: This standard was implemented on June 20, 2023.