Software Currency Policy Template

Why is DIR publishing this template?

One of the goals in the 2016-2020 State Strategic Plan for Information Resources encourages state agencies and institutions of higher education to “develop and adhere to a software currency policy that reduces the use of unsupported software and decreases security vulnerabilities in state agency IT systems.” Customers participating in the Data Center Services (DCS) Program are subject to a similar policy

How do I use this template?

This template is not a guideline for action at your agency. It is a starting point for developing internal policy and includes best practices for software currency.

This template is recommended for use by state agencies as a basis for the agency’s Software Currency Policy. Each agency must consider their tolerance and risk exposure for running unsupported software. Reference the DIR Policy Template and Examples found on the [DIR website](http://dir.texas.gov/View-Resources/Pages/Content.aspx?id=32) for additional information on writing policies.

Why do I need a Software Currency Policy?

A Software Currency Policy ensures executives, financial officers, and technical staff agree on the importance for up-to-date software and the cost and risk that is inherent in managing unsupported software products.

DIR recommends the agencies include software currency as an integral part of their technology roadmap. The roadmap should consider at minimum a three-year horizon to coincide with the state budget cycle and establish a plan and budget for upgrading software before it goes out of support and becomes high risk (i.e. security risk, disruption from loss of service).

Example Software Currency Policy Language

# Overview

Government has a responsibility to maintain vendor supported software across the agency to ensure the safety and security of software, systems, and data. All software eventually becomes out of support or unsupported depending upon the software development lifecycles. Continuing to use unsupported software constitutes a serious security risk.

# Scope

The policy applies to all software and related systems owned or maintained by the [AGENCY] (hereafter referred to as “agency”).

# Purpose

This policy is to ensure the agency maintains an up-to-date software portfolio to reduce the cost and risk inherent in managing unsupported software products. The term unsupported refers to software for which there are no longer commercial or vendor support options or software that relies on other unsupported applications or components.

# Policy

To ensure that the delivery of reliable, low risk, cost effective government services, the agency will reduce and, where possible, eliminate instances of unsupported software. The agency bears the full burden of risk associated with running unsupported software.

These risks include:

* increased cost to maintain a software asset, often referred to as “technical debt”
* lack of agility resulting from its inability to align with changes in business requirements
* limited capacity to integrate with up-to-date and cost competitive technologies (e.g. cloud)
* scarcity of skilled labor to maintain unsupported technologies
* increased mistakes and resulting costs from supporting the complexity of many versions across components

## Risk Assessment

In compliance with 1 TAC 202, the agency will conduct a high-level risk assessment of their software currency and either request necessary upgrades or replacement costs in their budget request, or determine the risk is tolerable based on system data, infrastructure, and vulnerability and business requirements. The assessment has a minimum three-year horizon and is updated at least once each fiscal year. Updates will be completed in time to include upgrade or replacement costs in the agency’s budget request.

If the agency chooses not to upgrade software prior to end of support the Executive Director must formally accept the risk of not doing so. End of support is the date when the vendor no longer provides automatic fixes, updates, or other technical assistance. Without vendor support, the software will no longer automatically receive security updates without additional costs.

## Replacement Schedule

The agency will plan to migrate off software that is designated by the vendor as upcoming end of support at least 12 months prior to that date. The agency must retire or replace any commercial off- the-shelf (COTS) software with a high or medium business impact before it reaches the end of support.

Vendors commonly announce software products end of support dates years in advance. Unlike the standard included mainstream support that is provided when a product is released and current, typically only security and reliability patches are available during the extended and end of support periods. No feature enhancements, architectural changes or warranties such as application backward compatibility, or new device drivers are offered once a product has gone out of mainstream standard support.

Replacement will be completed before software is out of support. Out of Support systems pose a significant liability and threat to the state. Out of Support software:

* no longer receives original manufacturer security updates that help protect State systems from all harmful viruses, spyware, and/or other malicious software that can harm or steal State data
* presents threats to interconnected State systems and data
* may not be compatible with current standard infrastructure

## Versioning

In software currency versioning, the current release version is known as N and the prior major version of the software as N-1. Older versions of software are labelled as N-2, N-3, etc. For the purposes of the software currency policy, N means the version of software designated and approved by the agency, as the current standard for deployment. N-1 is one release prior to the above-described designated or approved software version. N-2 is two or more releases prior to the above-described software version. Conversely, N+1 is any version level released by a manufacturer (in production or beta state) after the above-described N version.

N-1 should have at least 12 months remaining before being desiginated end of support or unsupported. Software that becomes version N-2 or greater is eligible for refresh and should be updated, replaced or discontinued with 12 months. If a refresh is not possible for technical or business reasons, an exception must be formally requested with statements that address the impacts on cost and security. Early adoption of N+1 release requires an exception to ensure it can be managed by the agency.

Note: Typically there is a gap between the latest current vendor software release and its designation by the agency as version N. This time allows for additional software testing, stability and preparedness by the agency for the upgrade.

# Definitions

**Software Currency** – the practice of maintaining the latest software for the deployed solution.

**End of Support –** the vendor no longer provides automatic fixes, updates, or other technical assistance. Without vendor support, the software will no longer receive security updates.

**Extended Support** – the period of time after end of support when the vendor may or may not offer addition software maintenance support at a cost for a period of time typically between one and five years.

**Mainstream Standard Support** - the period of time during which a vendor product is available for general release and receives warranty support, security and non-security updates.

**Out of Support Software –**  software that is no longer supported by software vendors except through customized or ad hoc support on a critical need only basis and for a fee. Vendors typically provide 3 years or more of warning before the actual out of support date.

**Refresh**- agency mechanism of updating software for currency. It is triggered by moving the version N to the next release.

**Unsupported Software –** refers to software for which there are no longer commercial, vendor, or in-house support options, or software that relies on other unsupported applications or components.

# References

* Texas Administrative Code: 1 TAC 202
* 2016-2020 State Strategic Plan for Information Resources Management

# Version History

Version 1.0 – Month XX, Year – Adopted policy.