End-of-Life Software Policy

Version Number	2.0
Last Approved	Feb 25, 2025
Classification	PUBLIC

Overview

Applicability

The applicability of this policy falls under purview of the Security Documentation Overview.

Purpose

This End-of-Life (EoL) Software Policy outlines the guidelines and procedures for managing software as it approaches the end of its lifecycle and provides guidelines on mandatory maintenance and updates until it's retired.

Scope

This End-of-Life Software Policy provides a framework to ensure that all products are receiving adequate attention and are regularly assessed for security fix viability and general supportability for our customers. This applies to all products across Company business lines, whether produced internally or with a third party.

End-of-Life (EoL) Software Policy

As a software solution reaches the end of its development cycle or has external components that are no longer supported, the Company recognizes that special consideration may be required to continue to offer and support a product for internal or customer use.

To ensure the integrity of our customers' data and to protect our systems, we must regularly review solutions for new vulnerabilities as they are discovered, which can change the risk profile

of the software solution. Business units must evaluate their ability to mitigate vulnerabilities, which may change the viability of the continued sale and support of the software solution.

As a product matures, the visibility and assessment of vulnerabilities are impacted by its development lifecycle. During active development, components are regularly examined by the development team in the process of building and compiling a solution.

As software enters a phase of stagnant development, teams must continue to adhere to security best practices, inclusive of patching operating systems, libraries, or third party component binaries, and adhere to software obsolescence timeframes of all tools, operating systems and libraries used to deliver the solution.

Lifecycle Definitions

Active Development and Sale

When a third party component has been identified as End-of-Life, an alternative solution must be implemented to continue to sell the product.

As tools used to produce, compile or build the solution reach “End-of-Life”, it is necessary that a port of the product must be done to an environment that continues to meet the standards of an active support lifecycle.

First Phase of Obsolescence

When a component used to deliver the solution is ending its life and an alternative has not been found and integrated, it is necessary to start phasing the component out or commit resources to refresh the product.

The **First Phase of Obsolescence** triggers a window of up to one year (or the end-of-support date of the software, whichever is sooner) to make appropriate determinations about a software solution’s future and should be thought of as an **evaluation and action period** to continued sustainability of a product.

Once an EoL scenario has been identified by the failure of meeting the following **requirements**, a product enters its **Sunset Phase**.

Requirements

- **OS** must continue to be patchable for the foreseeable future or the following decision must be made:
  a. Need to enter a **Sunset Phase** and develop an End-of-Life statement, or
  b. Engineering needs to port to a sustainable, supported OS.
- **Components** used within a solution must be:

    a. upgraded to a supported component version, or
    b. find and implement an alternative supported technology, or
    c. deprecate functionality dependent on the obsolete component.
- **Tools** used to generate a solution must continue to be supported such that a patch may be distributed at any time.

Sunset Phase

If a team chooses not to complete the remediations described in the **First Phase of Obsolescence**, the product immediately enters the **Sunset Phase**.

When triggered, the **Sunset Phase** requires:

- A definitive **End of Sale** date is published, which should be no longer than 6 months after the triggering component is out of support.
    - A renewal for existing customers may be possible so long as a final renewal date is no longer than the last support date.
- Sales teams should consider adjusting offerings to exclude the software solution from new sales and renewal quotes
- Active deals currently underway should set expectations with customers that no active development will be forthcoming
- Legal is involved in reviewing contracts for any termination obligations
- Advise customers that there is an alternative solution within the Company's portfolio, a third party solution, or state that there is no migration path to another solution
- Customer exports and migration must conclude before the end of support date, and
- Engineering teams must continue to make best effort to address any Severity 1 or Severity 2 vulnerabilities, but no further enhancement or non-critical bug fixes will be made
- Engineering shall freeze the components needed to build the product, which may require the use of obsoleted components
- Periodic penetration testing still needed as vulnerabilities may continue to evolve
- Sunsetted products will be tracked on the Company's Risk Register for visibility and will be continually evaluated for emerging risks

When a software solution reaches End-of-Life, the business will no longer address any vulnerabilities and will shut down all running instances.

Exceptions

Exceptions to this policy must be entered into the Company Risk Register and the Company's Exception Register and must be reviewed annually.

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @angelina.kilmer @Paul Gordon	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Feb 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History

Date	Author(s)	Version	Changes
Feb 25, 2025	@angelina.kilmer @Paul Gordon	2.0	Annual review
Nov 1, 2024	@angelina.kilmer	1.1	Changed Policy classification from Confidential to Public
Feb 21, 2024	@John Cole @Art Machado , Sarah Zwicker	1.0	Original version