

Policy Title and #	CIO-102: Technology Sunset Policy				
Effective Date:	07/08/2015	Revision Date:	11/16/2020	Review Date:	12/10/2020

POLICY STATEMENT:

This policy establishes controls addressing the sunseting of technology. The controls provide guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investments.

DEFINITION:

Technology Sunsetting - The business process in which the Commonwealth Office of Technology (COT), or an agency, determines and plans for the end of the useful life of a particular technology. Technologies are typically sunset when the technology is obsolete, unsupported or the function that required the technology is no longer needed due to changing business needs.

POLICY:

Obsolete or unsupported software and hardware present numerous risks to the Commonwealth, such as security vulnerabilities, incompatibility with features and functions of newer technologies and higher support costs. Consequently, this policy establishes the responsibilities for addressing technology in sunset status.

COT and agencies shall review their respective technology portfolios according to established review schedules, or at least every two years. The technology portfolio review should include participants responsible for IT asset management, finance/budgeting and IT standards such as information security, compliance and technical standards in order to ensure the technology meets then current security, business, and technology requirements and standards. If a technology cannot meet technology requirements and standards, or no longer meets business requirements, COT and the impacted agencies will collaborate to set a sunset date and plan for the removal of the technology from the environment.

For enterprise level technology or a technology that is an approved standard (Ex. KITS), If COT determines that such a technology needs to be sunset or replaced, COT shall notify agencies using an Agency Contact Memo (ACM). Agencies requesting an exemption for continued use of sunset enterprise technology or approved standard technology must submit an exception request to COT. The cost associated with retaining and supporting sunset technology is the responsibility of the agency, including any additional costs COT bears to support the sunset technology.

When an agency determines an agency-specific technology must be sunset, it shall inform the CIO and any potentially impacted agencies with a rationale for sunset status.

COT may disable any technology in sunset status if the CIO, after consultation with the CISO and the agency, determines the software creates a significant operational or security risk to the Commonwealth that warrants such action.

AUTHORITY:

KRS 42.726 authorizes the Commonwealth Office of Technology to develop policies and compliance processes to support and promote the effective applications of information technology within the executive branch of state government.

APPLICABILITY:

All executive branch agencies shall adhere to this policy. All non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

RESPONSIBILITY FOR COMPLIANCE:

Each agency shall ensure that all staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

MAINTENANCE:

COT's Office of IT Architecture and Governance is responsible for maintaining this policy. Organizations may modify this policy to fulfill their responsibilities, but must obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification.

REVIEW CYCLE:

COT will review this policy at least every two years.

REFERENCES:

Helpful references can be found on the Enterprise IT Policies webpage.