Policy Title and #	CIO-117: System and Services Acquisition				
Effective Date:	07/16/219	Revision Date:	11/05/2021	Review Date:	11/05/2021

POLICY STATEMENT:
This policy establishes controls related to System and Services Acquisition. The policy provides guidance in decision-making and practices that optimize resources, mitigate risk, and maximize return on investment.

POLICY:
The Commonwealth Office of Technology (COT) and other enterprise agencies with IT systems in the Commonwealth's infrastructure shall establish adequate security controls for the acquisition and deployment of agency information systems. COT establishes the minimum requirements for IT systems and services acquisition with the moderate-level access control standards outlined in the NIST Special Publication 800-53 Rev 4 System and Services Acquisition (SA) control family, in accordance with CIO-091 Enterprise Information Security Program.

Agencies shall adhere to the policies, procedures, and standards established by COT. For details on COT-approved controls, refer to the Office of the Chief Information Security Officer's (CISO) Enterprise Security Controls and Best Practices.

Agencies may request exceptions to this policy by submitting a security exemption request through ServiceNow. The CISO will consider requests on a case-by-case basis. COT may pass any costs resulting from the exemptions or exceptions to this policy to those agencies.

AUTHORITY:
KRS 42.726 authorizes the Commonwealth Office of Technology (COT) 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 and 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 staff within their organizational authority are made aware of and comply with this policy. The agency is responsible for enforcing this policy. Organizations may modify this policy to fulfill their responsibilities, but shall obtain approval through an exception request. Staff should refer to their internal policy, which may have additional information or clarification. 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 Contracts and Privacy is responsible for administrative coordination to maintain this policy, including review of this policy by the appropriate organizations at least every two years.

REFERENCES:

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