Policy Title and #	CIO-091: Enterprise Information Security Program				
Effective Date:	10/07/2013	Revision Date:	01/03/2019	Review Date:	04/21/2021

POLICY STATEMENT:
This policy establishes the Commonwealth's Enterprise Information Security Program.

POLICY:
The Commonwealth Office of Technology (COT), Office of the Chief Information Security Officer (CISO) shall establish and maintain an Information Security Program with concomitant policies to adopt security controls and standards to protect the Commonwealth's IT infrastructure, systems, and data.

The Office of the CISO will align the Commonwealth's security program with 18 specific control families of the security framework described in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The program shall establish policies and standards, using NIST's **moderate** impact controls, to address the following families of the NIST framework:

AC Access Control
AT Awareness and Training
AU Audit and Accountability
CA Security Assessment and Authentication
CM Configuration Management
CP Contingency Planning
IA Identification and Authentication
IR Incident Response
MA Maintenance
MP Media Protection
PE Physical and Environmental Protection
PL Planning
PM Program Management
PS Personnel Security
RA Risk Assessment
SA System and Services Acquisition
SC System and Communications Protection
SI System and Information Integrity

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 must adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government.

RESPONSIBILITY FOR COMPLIANCE:
Each agency must ensure that 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 the CISO 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's Office of the CISO will review this policy at least every two years.

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