COMMONWEALTH OFFICE OF TECHNOLOGY **Office of the Chief Information Officer Enterprise Policy (CIO)**		Page 1 of 2
CIO–091: Enterprise Information Security Program Policy		
EFFECTIVE DATE: 10/07/2013	**REVISED:** 01/03/2019 03/11/2024	**REVIEWED:** 04/21/2021 03/11/2024

I. PURPOSE

This policy establishes the Commonwealth’s Enterprise Information Security Program.

II. 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 5, *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 (no moderate impact controls for this family)
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

III. CORRECTIVE OR DISCIPLINARY ACTION

Each agency shall ensure that all relevant staff within their organizational authority are 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.

IV. 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. Organizations may modify this policy to fulfill their responsibilities but must obtain approval through an exception request. Staff should refer to their internal policy that may have additional information or clarification.

V. REFERENCES

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