Information Security Officer Policy

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
June 30, 2026

Supersedes:
ITP-SEC016

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Information Technology Policy (ITP) sets forth designation and responsibilities of an Information Security Officer (ISO).

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

4.1 Designation of Information Security Officer

Each agency shall designate an Information Security Officer (ISO) and direction is provided below on the designation of ISOs within Delivery Centers. This policy requires agencies to:

- Designate an Information Security Officer (ISO) and backup ISO
- Assign related roles and responsibilities
- Ensure separation of duties
- Support Agency and Enterprise collaboration
- Ensure adherence to the ISOs minimum responsibilities

4.1.1 Delivery Centers:

The Commonwealth Chief Information Security Officer (CISO) shall work in conjunction with the Delivery Center Chief Information Officer (CIO) and the Commonwealth CIO to designate a Commonwealth employee or Commonwealth contractor in the Delivery Center as the ISO. The designated individual will report directly to the CISO and be a member of the Enterprise Information Security Office. The Delivery Center ISO shall designate at least one backup for their role as ISO.

4.1.2 Independent Agencies:

Each independent agency CIO or designee shall identify and designate a Commonwealth employee or Commonwealth contractor in the agency as the ISO. The agency CIO or designee will notify the CISO, which individual(s) will assume the agency ISO role. When staff changes occur and the ISO role is reassigned, prompt notification of this change shall be submitted to the CISO. The agency CIO is strongly encouraged to designate at least one backup for the ISO.

4.1.3 Separation of Duties

Agencies shall ensure prevention measures are taken to avoid conflicts of interest and adhere to the security concept of separation of duties by assigning roles so that:

- The ISO is not a system owner or a Data Owner except in the case of compliance systems for information security
- The system owner and the Data Owner are not system administrators for IT resources or data they own
- The functions of ISO and Privacy Officer are assigned to different individuals as there are checks and balances in financial and health institutions where one individual executes and another audits the execution. It is important to have the individuals in these two roles check each other's activities to ensure that both information security and privacy policies are being carried out.

4.1.4 Information Security Officer Minimum Responsibilities

Individuals selected as ISO may be assigned multiple roles and responsibilities. The role and responsibilities shall allow adequate time and resources to fulfill ISO duties, provide adequate separation of duties and protect and prevent against the possibility of fraud or conflicts of interest.

The ISO's minimum responsibilities are, but not limited to:

- Developing and managing an agency information security program that meets or exceeds the requirements of Commonwealth IT security policies and standards in a manner commensurate with agency risk.
- Verifying and validating that all agency IT systems and data are classified for sensitivity in accordance with Commonwealth policies.
- Developing and maintaining an information security awareness and training program for agency staff, including contracted resources and IT service providers.
- Requiring that all Commonwealth authorized users complete required IT security

awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually thereafter pursuant with *Management Directive 535.09 Amended, Information Technology Security Trainings*.

- Implementing and maintaining the appropriate balance of preventative, detective, and corrective controls for agency IT systems commensurate with data sensitivity, risk, and systems criticality.
- Developing and documenting an agency security incident management process that aligns with the Office of Administration, Office for Information Technology (OA/IT) Cyber Security Incident Response Process. Refer to *IT Security Incident Reporting Policy* for guidance on agency reporting responsibilities and incident response procedures.
- Developing and executing an annual tabletop exercise of the agency's security incident management and response process. Provide an executive summary of the tabletop exercise to the agency CIO, agency Chief Technology Officer (CTO), and CISO. Refer to the Cyber Security Incident Response Process (IRP) for documentation on the Commonwealth's incident response procedures.
- Mitigating and reporting all cyber security incidents in accordance with this policy, and any other applicable ITPs, laws, statues or regulations (e.g., IRS Publication 1075, CJIS Security Policy, HIPAA, PCI, etc.), and CISO requirements. Ensuring appropriate actions are executed to prevent recurrence.
- Working with and communicating all IT security matters to the agency CTO and the agency CIO.
- Working with the Agency Privacy Officer to ensure all privacy requirements are met. Determining the sensitivity of the data created or processed within the organization and establishing and defining appropriate controls and acceptable levels of risk.
- Ensuring appropriate organizational security procedures and standards are in place to support and align with the agency and Commonwealth policies, procedures, or standards, as well as any regulatory requirements (e.g., IRS Publication 1075, CJIS Security Policy, HIPPA, PCI, etc.).
- Coordinating the implementation of detection, correction, or preventative information security measures as necessary.
- Providing assurance to management and the CISO that the organization complies with legislative, contractual, regulatory, and Commonwealth policy requirements regarding information security.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the enterprise IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document