Information Technology Policy

Information Security Officer Policy

Number ITP-SEC016	**Effective Date** March 29, 2006
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** December 2024

1. Purpose

This Information Technology Policy (ITP) mandates that each agency designate an Information Security Officer (ISO) and provides direction on the designation of ISOs within Delivery Centers. In addition, it provides guidance on the assignment of roles and responsibilities of that individual.

2. Scope

This ITP 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 ITP as outlined in the Responsibilities section.

3. Policy

This ITP establishes an enterprise-wide policy for the identification of an Information Security Officer. 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

3.1 Designation of Information Security Officer

3.1.1 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.

3.1.2 Independent Agencies

Each independent agency CIO or designee shall identify and designate a Commonwealthemployee 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.

3.2 Assignment of Roles & 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.

3.3 Separation of Duties

Agencies shall ensure prevention measures are taken to avoid conflict of interests 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; and

- 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.

3.4 Agency and Enterprise Collaboration

The ISO shall have the capability and authority to raise concerns, issues, and report problems and cyber security incidents to the CISO via the chain of command.

3.5 Information Security Officer Minimum Responsibilities

The ISO is responsible for developing and managing the agency's information security program. The ISO's minimum responsibilities are as follows, but not limited to:

- Develop and manage 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.

- Verify and validate that all agency IT systems and data are classified for sensitivity in accordance with Commonwealth policies.

- Develop and maintain an information security awareness and training program for agency staff, including contracted resources and IT service providers. Require 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*.

- Implement and maintain the appropriate balance of preventative, detective, and corrective controls for agency IT systems commensurate with data sensitivity, risk, and systems criticality.

- Develop and document 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 *ITP-SEC024, IT Security Incident Reporting Policy* for guidance on agency reporting responsibilities and incident response procedures.

- At least once annually, develop and execute a 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.

- Mitigate and report all cyber security incidents in accordance with *ITP-SEC024, IT Security Incident Reporting Policy*, and any other applicable ITPs, laws, statues or regulations (e.g., IRS Publication 1075, CJIS Security Policy, HIPAA, PCI, etc.), and CISO requirements. Ensure appropriate actions are executed to prevent recurrence.

- Work with and communicate all matters related to IT security to the agency CTO and the agency CIO.

- Work with the agency Privacy Officer to ensure all privacy requirements are met. Determine the sensitivity of the data created or processed within the organization and establish and define appropriate controls and acceptable levels of risk.

- Ensure 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.).

- Coordinate the implementation of detection, correction, or preventative information security measures as necessary.

- Provide management and the CISO assurance that the organization complies with legislative, contractual, regulatory, and Commonwealth policy requirements regarding information security.

4. Responsibilities

4.1 Agencies and designated ISOs shall:
Comply with the requirements as outlined in this ITP.

4.2 OA/IT shall:
Comply with the requirements as outlined in this ITP.

4.3 Third-party vendors, licensors, contractors, or suppliers shall:
Provide contact information for an ISO and backup ISO who is responsible for all security matters related to the Commonwealth account.

5. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 535.09 Amended, Information Technology Security Trainings*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC019, Policy & Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC024, IT Security Incident Reporting Policy*
- *ITP-PRV002, Electronic Information Privacy Officer*
- *Cyber Security Incident Response Process (IRP)* *(Commonwealth Access Only)*
- *Internal Revenue Service Publication 1075*
- *CJIS Security Policy*

6. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

7. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

8. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	03/29/2006	Base Policy	N/A
Revision	05/12/2012	Refresh	N/A
Revision	04/02/2014	ITP Reformat	N/A
Revision	03/16/2017	• Added Exemption section. • Removed unnecessary language. • Removed agency Deputy Secretary of Administration responsibility of identifying agency Information Security Officer • Revised the Policy section for clarity. • Added additional ISO minimum responsibilities	N/A
Revision	09/22/2022	• ITP Refresh • Added policy links/updated references to homepages per Legal direction. • Added third party vendor language to Scope and Responsibilities. • Added references to CJIS and IRS in Reference section. • Basic terminology updates for abbreviations throughout • Updated usage of word appointment/appoint to designation or designate. • Added policy language to account for DC ISO positions. • Added section 3.2 for roles and responsibilities and placed existing policy language within the new section. • Scope language updated to require any entity connecting to the commonwealth network to follow ITP.	N/A
Revision	12/01/2023	• Annual review. • Added bulleted list summarizing policy requirements. • Grammatical and organizational updates • Under Section 3.5 requirement added for annual tabletop exercises. • Added requirement to ensure all privacy requirements are met with references to HIPAA, CJIS and IRS Publication 1075. • Removed duplicative language regarding ensuring organizational security procedures align with OA/IT policies procedures, and standards removed. • Reference added to IRP under Related ITPs/Other References.	Revised IT Policy Redline <12/01/2023>