pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Commonwealth of Pennsylvania – Information Security Officer Policy

ITP Number ITP-SEC016	**Effective Date** March 29, 2006
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** March 2018

1. Purpose

The purpose of this Information Technology Policy (ITP) is to mandate that each agency appoint an Information Security Officer (ISO), and to provide guidance on the appointment and responsibilities of that individual.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Policy

This ITP establishes an enterprise wide policy for the identification of an Information Security Officer. This policy requires agencies to:

Appointment.

- Each agency Chief Information Officer (CIO) or designee is to identify and designate a Commonwealth of PA employee or Commonwealth contractor [by name and title] in the agency as the Information Security Officer (ISO).
- The agency CIO is strongly encouraged to designate at least one backup for the ISO. Also, individuals selected may be assigned multiple roles and responsibilities, if the role and responsibilities allow adequate time and resources to fulfill ISO duties, provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to conflicts of interest.
- The agency CIO or designee will notify the Office of Administration, Office for Information Technology - Chief Information Security Officer (OA/OIT - CISO), which individual(s) will assume the agency Information Security Officer role. When staff changes occur and the Information Security Officer role is reassigned, prompt notification of this change is to be submitted to the OA/OIT CISO.

Separation of Duties.

- Prevent or have designee prevent 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 systems, network infrastructure, or data they own; and
- Assign the functions of Information Security Officer and Privacy Officer 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.

Agency and Enterprise Collaboration.
The agency Information Security Officer shall have the capability and authority to raise concerns, issues, and report problems and cyber security incidents to the OA/OIT – CISO via chain of command.

Information Security Officer Minimum Responsibilities:
The ISO is responsible for developing and managing the agency's information security program. The ISO's duties 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 risk.

- Verify and validate that all agency IT systems and data are classified for sensitivity.

- Develop and maintain an information security awareness and training program for agency staff, including contractors and IT service providers. Require that all COPA IT system 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.

- 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 OA/OIT security incident management process. Refer to ITP-SEC024 IT Security Incident Reporting Policy for guidance.

- Mitigate and report all IT security incidents in accordance with Commonwealth IT Policy, applicable laws and CISO requirements and take appropriate actions to prevent recurrence.

- Work with and communicate all matters related to IT security to the agency Chief Technology Officer and the agency Chief Information Officer. The individual shall work with their agency's Privacy Officer to ensure that all privacy requirements are met.

- Work with the agency Privacy Officer to determine the sensitivity of the data created and/or processed within the organization and establish and/or define appropriate controls and acceptable levels of risk.

- Ensure appropriate organizational security procedures and standards are in place to support the agency and commonwealth information security policy and any regulatory requirements.

- Coordinate the implementation of detective, corrective, or preventative information security measures as necessary and provide management and the OA/OIT CISO assurance that the organization complies with legislative, contractual, regulatory, and Commonwealth policy requirements regarding information security.

- Ensure organizational security procedures align with OA/OIT information technology policies/procedures/standards.

6. Responsibilities

Agencies and appointed Information Security Officers are required to perform the actions outlined in this policy.

7. Related ITPs/Other References

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

- ITP-SEC000 *Information Security Policy*
- ITP-SEC024 *IT Security Incident Reporting Policy*
- ITP-PRV002 *Electronic Information Privacy Officer*
- Internal Revenue Service Publication 1075

8. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

9. Publication Version Control

It is the 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 are to be directed to RA-ITCentral@pa.gov.

10. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	03/29/2006	Base Policy
Revision	05/12/2012	Refresh
Revision	04/02/2014	ITP Reformat
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