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 Recommended Policy	***Supersedes***
Contact RA-ITCentral@pa.gov	***Scheduled Review*** Annual

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

1. Purpose

The purpose of this Information Technology Policy (ITP) is to mandate that each agency appoint an Information Security Officer, 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:

- Identify and designate a Commonwealth of PA employee [by name and title] in the agency as the Information Security Officer. The designated individual shall work closely with and communicate all matters related to IT security to the Agency Chief Technology Officer and/or the agency Chief Information Officer. It is recommended that the person responsible for information security work closely with their agency Privacy Officer, to ensure that all security and privacy requirements are met.

- Assign the functions of Information Security Officer and Privacy Officer to different individuals. The rationale for having them separate is that the roles, while on the surface appearing to be very similar, in fact have different purposes, which at times may be in conflict. As there are checks and balances in the financial world where one person executes and another audits the execution, so too it is important to have the individuals in these two roles check each other's activities to be sure that both information security and privacy policies are being carried out.

- Empower the agency Information Security Officer to raise his/her concerns and/or report problems and cyber security incidents to the Office of Administration/Office for Information Technology - Chief Information Security Officer (OA/OIT - CISO).

- Each agency Deputy Secretary for Administration or designee is to identify and notify the OA/OIT CISO, which individual(s) will assume the agency Information Security Officer role. If and 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

Information Security Officer Minimum Responsibilities:

- 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 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 security policies/procedures/standards

6. Responsibilities

Agencies are required to perform the actions outlined in this policy.

7. Related ITBs/Other References

8. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

9. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

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

Version	Date	Purpose of Revision
Original	3/29/2006	Base Policy
Revision	5/12/2012	Refresh
	4/2/2014	ITP Reformat