pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

# Information Technology Policy

## *Information Security Policy*

| **ITP Number**<br>ITP-SEC000 | **Effective Date**<br>May 2016 |
|---|---|
| **Category**<br>Security | **Supersedes**<br>None |
| **Contact**<br>RA-ITCentral@pa.gov | **Scheduled Review**<br>Annual |

## 1. Purpose

This Information Security Policy is necessary to ensure that the Commonwealth of PA:

- Establishes an enterprise-wide approach to information security, including appropriate security awareness training, and education.
- Complies with federal and state guidelines and regulations regarding the collection, maintenance, use, and security of information resources.
- Provides a mechanism for agencies to collaborate with the Office of Administration, Office for Information Technology on new and emerging technologies in order to effectively develop and share enterprise and security architecture deliverables by:
    - Establishing and implementing prudent, reasonable, and effective practices for the protection and security of information resources which includes the protection of sensitive and confidential information against accidental or deliberate unauthorized disclosure, modification, or destruction.
    - Developing effective mechanisms for responding to incidents, breaches or misuse of commonwealth IT assets and of information security policy.
    - Providing a minimum level of Information Technology (IT) security requirements which have been determined acceptable for the transmission, processing, and storage of sensitive system data and business processes.
    - Reducing the overall and specific risk of breach or misuse of commonwealth IT assets and the associated damage and cost of breach or misuse.

This policy establishes a program to ensure that the commonwealth meets or exceeds its legal and ethical responsibilities for securing its critical and sensitive information assets. Information Technology Policies (ITPs) are IT-related policies that apply to agencies, boards and commissions under the Governor's jurisdiction. ITPs direct organizations to engage or avoid specific practices and/or specify enterprise product standards.

## 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. Definitions

**3.1 Commonwealth of PA Procurement and Architectural Review (COPPAR):** The review mechanism the Office for Information Technology uses to review agency requests for policy waivers and large IT-related procurements

**3.2 Enterprise Information Security Office (EISO):** Office within the Office of Administration, Office for Information Technology tasked with managing the enterprise IT security posture for the commonwealth as it pertains to governance, risk, and compliance.

**3.3 Federal Information Processing Standards (FIPS):** A federal IT standard established by the National Institute of Standards and Technology

**3.4 National Institute of Standards and Technology (NIST):** A division of the federal Department of Commerce tasked with research and, including establishment of federal IT standards

## 4. Policy

The Office of Administration, Office for Information Technology (OA/OIT) is responsible for protecting the Commonwealth's information assets in accordance with all applicable federal and state guidelines and regulations; as well as, with effective information security practices and principles generally accepted as "due diligence" within the business community.

All agencies must comply with Commonwealth Information Security Policies. Information Security Policies are identified as Information Technology Policies (ITPs) by the Security (SEC) designation.

Appropriate action will be taken when loss, damage, or breach of confidentiality results from non-compliance with commonwealth policies and Management Directives. Any agencies found to be in non-compliance with Commonwealth ITPs must employ immediate corrective actions. Agencies must also have compliance and risk management methodology in place to ensure agencies are maintaining compliance, remediating vulnerabilities and reducing IT security risk.

In lieu of existing policies or procedures that cover new or existing security implementation, the commonwealth will follow industry security best practices and/or well-known security standards such as the Federal Information Processing Standards (FIPS) and Special Publications (SP) published by the National Institute of Standards and Technology (NIST). If there is not a security ITP that covers the scope of the security implementation, agencies must submit a waiver for this policy accompanied by the specific proposed solution through the COPPAR system for review by EISO.

## 5. Related ITPs / Other References

- National Institute of Standards and Technology (NIST) Special Publications (SP) - http://csrc.nist.gov/publications/PubsSPs.html
- Federal Information Processing Standards Publications (FIPS PUBS) - http://csrc.nist.gov/publications/PubsFIPS.html

## 6. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

## 7. 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.

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

| Version | Date | Purpose of Revision |
|---|---|---|
| Original | 05/19/2016 | Base Document |