pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Information Security Policy

Number ITP-SEC000	**Effective Date** May 2016
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** July 2024

1. Purpose

This Information Technology Policy (ITP) establishes a program to ensure that the Commonwealth meets or exceeds its legal and ethical responsibilities for securing its IT Resources including, but not limited to, its critical and sensitive information technology resources. This ITP is necessary to ensure that the Commonwealth:

- 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 IT Resources.

- Provides a mechanism for agencies to collaborate with the Office of Administration, Office for Information Technology (OA/IT) on new and emerging technologies 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 IT Resources, which includes the protection of sensitive and confidential information against accidental or deliberate unauthorized disclosure, modification, or destruction.

    - Developing information security policies and effective mechanisms for responding to incidents, breaches, or misuse of IT Resources.

    - Providing a minimum level of Information Technology (IT) security requirements that have been determined acceptable for the transmission, processing, and storage of sensitive system data and business processes.

    - Reducing the overall and specific risks of breach or misuse of Commonwealth IT Resources and the damages and costs associated with a breach or misuse.

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

OA/IT is responsible for protecting the Commonwealth's IT Resources 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.

Agencies must comply with Commonwealth Information Security Policies. Information Security Policies are identified as 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. Agencies found to be in non-compliance with 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 risks.

In the absence 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 FIPS and Special Publications (SP) published by the 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 policy waiver process for review by the Enterprise Information Security Office (EISO). Refer to Section 9 and *ITP-BUS004, IT Waiver Review Process* for guidance on the policy waiver process.

3.1 Offshore Access

Offshore access to Commonwealth production systems, whether hosted by the Commonwealth or by third parties, is prohibited by anyone not physically located in CONUS. This includes, but is not limited to:

- Virtual Private Network (VPN);
- Remote desktop;
- Virtual Desktop Infrastructure (VDI);
- Cloud infrastructure such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings; and
- All access to Commonwealth "C" designated data, as defined in ITP-SEC019, *Policies and Procedures for Protecting Commonwealth Electronic Data*.

Authorized Users are prohibited access to all Commonwealth IT Resources and data from countries which are blocked by the Enterprise GeoIP service in accordance with *ITP-SEC034, Enterprise Firewall Rule Set*.

It is required that all Commonwealth "C" designated data, as defined in *ITP-INF015,* *Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*, reside in CONUS where it is subject to the laws and regulations of the United States and the various jurisdictions within the United States. Transmission to Offshore systems or storage on Offshore systems is prohibited.

1) Offshore direct remote access to "C" designated data on any Commonwealth production system is prohibited regardless of the file type or storage medium. This includes, but is not limited to:
   - Databases;
   - Documents (PDF, Word, Text, etc.);
   - Spreadsheets; and
   - Images.

2) Offshore direct remote access to networking equipment (including but not limited to routers, switches, firewalls, etc.) which could be changed to gain access to "C" designated data on any internal system in the Commonwealth is prohibited.

Offshore work will be strictly limited to lower and test environments. There shall be no offshore access to production servers or to production environments. Offshore resources will only receive test or anonymized data that is not traceable or linkable to "C" designated data. Offshore resources should have no access to production data.

Offshore work should be performed in accordance with the *OPD-SEC000A, Security Requirement Traceability Matrix (Commonwealth access only).* All maintenance and support after system implementations should be performed by resources located and authorized to work within CONUS. Offshore resources should not be used for any post go live support.

4. Responsibilities

4.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

4.2 Office of Administration, Office for Information Technology shall:

Comply with the requirements as outlined in this ITP.

4.3 Third-party vendors, licensors, contractors, or suppliers shall:

- Ensure compliance with the requirements outlined in *OPD-SEC000B, Security Policy Requirements for Third Party Vendors*.
- Ensure the location(s) of its servers and data center(s) as well as the location of the workforce accessing them are within the United States of America.
- Ensure IT environments and systems that contain Commonwealth data comply with all Commonwealth ITPs, as changes and revisions are made to reflect alignment with the most current Commonwealth ITPs.

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*
- *OPD-SEC000A, Security Requirement Traceability Matrix (Commonwealth access only).*
- *OPD-SEC000B, Security Policy Requirements for Third Party Vendors*
- *ITP-SEC034, Enterprise Firewall Rule Set*
- *ITP-SEC019, Policies and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-PLT012, Use of Privately Owned PCs to Access COPA Resources*
- *National Institute of Standards and Technology (NIST) Special Publications (SP)*
- *Federal Information Processing Standards Publications (FIPS PUBS)*

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	05/01/2016	Base Document	N/A
Revision	05/07/2020	Clarified language throughout. Revised Definitions section Added Exemption section. Removed references to COPPAR throughout Offshore Access added. OPD-SEC00A Security Requirement Traceability Matrix created	N/A
Revision	05/27/2022	ITP Refresh Links updated. Third party language added. Responsibilities updated for Third parties.	N/A

Version	Date	Purpose of Revision	Redline Link
Revision	07/18/2023	Definitions replaced with links to glossary. Scope updated based on connecting to COPA network and to add third party requirement as outlined in Responsibilities. Updated third party responsibilities section to include statement on OPD-SEC000B. Additional policy language added to reference ITP-SEC034 and prohibit access to Commonwealth IT resources/data.	Revised ITP Policy Redline <07/18/2023>