pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Virtualization Policy

ITP Number ITP-SYM008	**Effective Date** November 20, 2009
Category Systems Management	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** December 2020

1. Purpose

Establishes virtualization policy and standards for the Commonwealth.

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 Guest Operating System: An operating system that runs inside the virtualization application. It is also referred to as a virtual machine (VM).

3.2 Host Operating System: The underlying operating system is installed on the physical system and used to manage the virtual environment.

3.3 Network management entities: Internal or external agencies or Commonwealth-contracted vendors tasked with management of commonwealth IT networks.

3.4 Sponsoring agency: Commonwealth agency in contract with external network management entity.

4. Policy

New projects implementing the use of virtualization technologies are to adhere to the policy and standards contained in this ITP. If an agency is considering utilizing virtualization for a server farm, it is recommended that a baseline be performed and that a cost/benefit analysis be conducted. Information obtained from the baseline and cost/benefit analysis is to be made available to other agencies. Typical baseline generation is to be conducted over a two-to-four-week period and is to track statistics including: CPU, memory, disk, and networking utilization.

Agencies that desire virtualization products for enterprise mission-critical servers requiring high availability are to complete an IT Procurement Request (detailed in ITP-BUS002 *IT Investment Review Process)* and submit it to the appropriate agency CoP planner.

Note: This ITP defines mission-critical servers as systems that require 100 percent guaranteed support and significant liability to maintain business continuity is placed on the supporting vendor(s). Not all independent software vendors (ISVs) will commit to providing support for their products running in a virtualized environment. Obtaining full ISV problem resolution services for ISV products running in a virtualized environment may require agencies to recreate the problem in a non-virtualized environment. Agencies are to factor criticality of the application, ISV support terms and conditions, and plan problem resolution procedures into the decision to execute an application in a virtualized environment.

Network management entities may employ virtualized network technologies (MPLS, VRFs, VLANs, SDN, VxLANs, and similar virtual technologies) to maintain multiple security and routing instances. Entities wishing to connect shall implement the following controls:

- The entity shall not provide interconnection between Security Zones of the Commonwealth network.
- The entity shall ensure that all non-Commonwealth connectivity and/or traffic be isolated from all Commonwealth Security Zones
- The entity shall ensure that proper separation of the various Commonwealth Security Zones is maintained between virtual network(s) and virtual host(s).
- The entity shall provide Office of Administration, Office for Information Technology, Enterprise Information Security Office (OA/OIT/EISO) with auditability to ensure that proper network segmentation is maintained.
- Except where permission is explicitly granted (via an approved IT policy waiver) by the EISO, the entities shall not permit leaking of traffic information from one Commonwealth security zone to another via any means.
- Traffic between security zones must only be permitted when it traverses an approved network security gateway device with a rule-base maintained by a Commonwealth authorized gateway management organization operating with the explicit permission and under the security oversight of EISO.
- If there is a special business need to provide this functionality (ex: route leaking for device management) beyond the existing approved gateway management team(s), the entity must have its sponsoring agency submit the appropriate IT policy waiver request and obtain approval before implementing such a configuration.
- Requests for network configurations, including firewall reconfigurations should be submitted following the Service Request process. This process is detailed at: https://itcentral.pa.gov/Pages/Enterprise-Services.aspx (*CWOPA Limited Access*).

5. Responsibilities

Commonwealth Agencies are to utilize the virtualization solutions detailed in OPD-SYM008A *Virtualization Standards*.

6. 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

- Management Directive 205.34 *Commonwealth IT Acceptable Use Agreement*
- OPD-SYM008A *Virtualization Standards*
- ITP-BUS004 *IT Waiver Review Process*
- ITP-BUS002 *IT Investment Review Process*
- Office of Administration, Office for Information Technology (OA/OIT) Service Request process: https://itcentral.pa.gov/Pages/Enterprise-Services.aspx (*CWOPA Limited Access*)

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

8. 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.

9. Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT 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
Original	11/20/2009	Base Document	N/A
Revision	12/20/2010	ITP Refresh	N/A
Revision	12/03/2019	ITP Reformat Renamed ITP Title, dropped "Server" Removed "Problem Statement and Solution Statement" and "Background" subsections Created OPD-SYM008A for Product Standards	Revised IT Policy Redline <12/03/2019>