pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise Security Auditing and Monitoring
Internet Access Control and Content Filtering Standard

ITP Number	**Effective Date**
ITP-SEC003	August 8, 2012
Category	**Supersedes**
Security	--
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	March 2019

1. Purpose

Policy on the use of an internet access control and content filtering solution that allows the commonwealth to block access to internet sites and content which pose a risk to the security of the network.

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. Objective

To establish the standards for use of the commonwealth's internet access control and content filtering (IACCF) solution for controlling and filtering internet traffic.

4. Policy

All internet traffic will be directed through the CoPA IACCF implementation. The standard solution is detailed in section 5, Product Standards for IACCF, in this ITP. All entities utilizing commonwealth internet access are required to submit a waiver if business requirements conflict with the overall CoPA IACCF implementation, minimum filtering policies detailed in section 6, Minimum Configuration Requirements for IACCF in this ITP. Additionally, all entities are to follow the change management process to request filtering policy changes.

If an agency under the governor's jurisdiction is using a similar solution from a different vendor, the agency is to leverage the CoPA Enterprise IACCF implementation for internet monitoring and filtering upon expiration of its current contract.

5. Product Standards for IACCF

CURRENT STANDARDS

(These technologies meet the requirements of the current architecture and are recommended for use.)

Technology	Platforms	Category
Current Telecom Service/Product Offerings	Current Telecom Service/Product Offerings	Web Filtering Solution

CONTAIN

(These technologies no longer meet the requirements of the current architecture and are not recommended for use. They are to be phased out over time. No date has been set for their discontinuance.)

Technology	Platforms	Category
--	--	--

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards. They are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request. Research technologies are less widely accepted, and time will determine if they will become a standard.)

Technology	Platforms	Category
--	--	--

6. Minimum Configuration Requirements for IACCF

The purpose of the IACCF Minimum Configuration is to protect commonwealth assets and enforce the Commonwealth Acceptable Internet Use policy by preventing HTTP(s) access to sexually explicit sites, spyware/malware related sites, and content that poses significant risk to commonwealth IT resources. The minimum requirement consists of a Disallow rule for the following categories. Each category has a specific exemption process that is documented in the configuration table. Refer to Section 11 Exemption from This Policy for specific details on the processes.

Enterprise minimum blocking configuration:

Category	Description	Exemption Process
Child Abuse	Websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at http://www.iwf.org.uk.	COPPAR
File Sharing and Storage	Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos. Products or services designated this category and listed in the Enterprise Service Catalog are exempt from this policy and do not require a COPPAR waiver to deploy.	COPPAR
Malicious Websites	Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse.	COPPAR

Category	Description	Exemption Process
Hacking	Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites	COPPAR
Other Adult Materials	Mature content websites (18+ years and over) that feature or promote sexuality, strip clubs, sex shops, etc. excluding sex education, without the intent to sexually arouse.	COPPAR
Peer-to-Peer File Sharing	Websites that allow users to share files and data storage between each other.	COPPAR
Dating	Websites that allow individuals to make contact and communicate with each other over the Internet, usually with the objective of developing a personal, romantic, or sexual relationship.	COPPAR
Phishing	Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.	COPPAR
Pornography	Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.	COPPAR
Proxy Avoidance	Websites that provide information or tools on how to bypass Internet access controls and browse the Web anonymously, includes anonymous proxy servers.	COPPAR
Remote Access	Sites that facilitate authorized access and use of computers or private networks remotely across the internet.	COPPAR
Spam URLs	Sites that are part of the spam ecosystem, including sites linked in unsolicited bulk electronic messages and sites used to generate or propagate such messages.	COPPAR
Streaming Internet Television, Radio, or Movie Services	Internet websites and applications associated with providing paid or unpaid streaming television, radio, or movie content.	COPPAR
Non-approved URL (Link) Shortening Services	Internet services that generate shortened URL's and redirect the user to the original longer URL's	COPPAR
Cloud Management Hosting/App Dev Services	Sites that offer the ability to manage and develop off-premise based application development & hosting services, including but not limited to, Microsoft Azure, Amazon Web Services (AWS), Go-Daddy, and Rackspace.	Service Request

Enterprise URL Denied and Allowed Rule Set

The Enterprise Information Security Office (EISO) will maintain OPD-SEC003A *Enterprise URL Deny/Allow Rule Set* which agencies and delivery centers must comply with. This operating document specifies which public URLs are allowed or not allowed access to from the

commonwealth network.

Agencies or delivery centers needing access to "Denied" URLs for business requirements must submit a COPPAR ITP waiver request against this policy. If approved the waiver is to be submitted as part of a Service Request to Allow the URL for the specific agency or delivery center.

Agencies may create any amount of more "Deny" (but not "Allow") rules per business requirements that are not identified in OPD-SEC003A.

7. Responsibilities

Commonwealth's Chief Information Security Officer (CISO) will regularly audit entity filtering policies for compliance with this policy and its associated standards.

Agency/Delivery Center Information Security Officers (ISOs) or designates are to ensure are to ensure agency/delivery center internet traffic is in accordance with this policy.

8. 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

- OPD-SEC003A *Enterprise URL Deny/Allow Rule Set (obtain from Enterprise Information Security Office EISO)*
- ITP-SEC000 *Information Security Policy*
- ITP-SEC024 *IT Security Incident Reporting Policy*

9. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

10. 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.

11. Exemption from This Policy

- **COPPAR:** 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 on IT Central at https://itcentral.pa.gov. Agency CIO approval is required.

- **Service Request:** In the event an agency chooses to seek an exemption for categories identified in Section 6 that require the OA/OIT Service Request process, please follow the procedures outlined in the Service Request process document located at: https://itcentral.pa.gov/Pages/Enterprise-Services.aspx (limited access).

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

Version	Date	Purpose of Revision
Original	01/18/2007	Base Document
Revision	08/30/2012	Standard Refresh
Revision	04/02/2014	ITP Reformat; Merged OPD-SEC003B, STD-SEC003A into ITP
Revision	10/29/2014	Updated COPPAR acronym
Revision	05/07/2015	In Section 6, added language/mandatory exception table requiring agencies to allow unrestricted access to a number of URLs
Revision	01/06/2016	In Section 6, added language/mandatory exception table requiring agencies to allow unrestricted access to a number of URLs
Revision	03/07/2017	Added "Cloud Management Hosting / App Dev Services" category to Section 6 configuration table Added Exemption Process to Section 6 configuration table Added Exemption section detailing COPPAR and Service Request processes
Revision	03/19/2018	Added OPD-SEC003A Enterprise URL Deny/Allow Rule Set Revised Enterprise Minimum Blocking Configuration Table Removed Retire Product table