pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Enterprise Content Filtering Standard

ITP Number ITP-SEC003	**Effective Date** August 8, 2012
Category Security	**Supersedes** --
Contact RA-ITCentral@pa.gov	**Scheduled Review** July 2022

1. Purpose

This Information Technology Policy (ITP) establishes guidance 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 ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Policy

All internet traffic will be directed through the Commonwealth's Internet Access Control and Content Filtering (IACCF) implementation. All entities utilizing Commonwealth internet access are required to submit an IT policy waiver if business requirements conflict with the IACCF implementation minimum filtering policies as detailed in section 4, Minimum Configuration Requirements for IACCF. All entities are to follow the change management process to request filtering policy changes.

HTTPS inspection of outbound internet traffic is enabled for most content filtering service categories except for those IACCF Categories identified in section 5, which are not inspected due to the sensitivity of the internet access. The decryption of HTTPs traffic allows security tools to analyze traffic for threats and block them.

If an agency under the Governor's jurisdiction is using a similar solution from a different vendor, the agency shall leverage the Commonwealth Enterprise IACCF implementation for internet monitoring and filtering upon expiration of the agency's current contract. Refer to OPD-SEC003A *Enterprise URL Deny/Allow Rule Set* (*Authorized COPA personnel only)* for IACCF product standard information.

4. Minimum Configuration Requirements for IACCF

The minimum requirements consist of a disallow rule for the following categories. Each category has a specific exemption process that is documented in the configuration table. Refer to the Exemption section for guidance.

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.	Policy Waiver
Discrimination	Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.	Policy Waiver
Explicit Violence	This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc.	Policy Waiver
Extremist Groups	Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs.	Policy Waiver
Illegal or Unethical	Websites that feature information, methods, or instructions on fraudulent actions or unlawful conduct (non-violent) such as scams, counterfeiting, tax evasion, petty theft, blackmail, etc.	Policy Waiver
Nudity and Risqué	Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse.	Policy Waiver
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 in this category and listed in the Enterprise Service Catalog are exempt from this policy.	Policy Waiver
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 a virus or trojan horse.	Policy Waiver
Hacking	Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites	Policy Waiver
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.	Policy Waiver
Peer-to-Peer File Sharing	Websites that allow users to share files and data storage between each other.	Policy Waiver
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.	Policy Waiver
Phishing	Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.	Policy Waiver
Pornography	Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.	Policy Waiver
Proxy Avoidance	Websites that provide information or tools on how to bypass internet access controls and browse the Web anonymously, includes anonymous proxy servers.	Policy Waiver
Remote Access	Sites that facilitate authorized access and use of computers or private networks remotely across the internet.	Policy Waiver

Category	Description	Exemption Process
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.	Policy Waiver

Domains/URL's blocked per OPD-SEC003A	Description	Exemption Process
Specific Streaming Internet Television, Radio, or Movie Services	Internet websites and applications associated with providing paid or unpaid streaming television, radio, or movie content.	Policy Waiver
Specific Non-approved URL (Link) Shortening Services	Internet services that generate shortened URL's and redirect the user to the original longer URL's	Policy Waiver
Specific Cloud Management Hosting/App Dev Services	Sites that offer the ability to manage and develop off-premise based application development & hosting services.	Service Request

Enterprise URL Denied and Allowed Rule Set

The Enterprise Information Security Office (EISO) shall maintain OPD-SEC003A *Enterprise URL Deny/Allow Rule Set* that agencies must comply with. This operating document specifies which public URLs are allowed or not allowed to be accessed from the Commonwealth network.

Agencies needing access to Category "Denied" URLs for business requirements shall submit an IT policy 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.

Agencies may create more Category "Deny" (but not "Allow") rules for business requirements that are not identified in OPD-SEC003A.

5. Enterprise Categories not HTTPs inspected due to the sensitivity of the internet access.

Category	Description
Finance and Banking	Financial Data and Services: Sites that offer news and quotations on stocks, bonds, and other investment vehicles, investment advice, but not online trading. Includes banks, credit unions, credit cards, and insurance. Mortgage/insurance brokers apply here as opposed to Brokerage and Trading.
Government and Legal Organization	Government: Sites sponsored by branches, bureaus, or agencies of any level of government, except for the armed forces, including courts, police institutions, and city-level government institutions. Legal Organizations: Sites that discuss or explain laws of various government entities.

Brokerage and Trading	Sites that support active trading of securities and management of investments. Real estate broker does not apply here and falls within Shopping and Auction. Sites that provide supplier and buyer info/ads do not apply here either since they do not provide trading activities.
Personal Privacy	Sites providing online banking, trading, health care, and others that contain personal privacy information.

Category	Description
Health and Wellness	Sites that provide information or advice on personal health or medical services, procedures, or devices, but not drugs. Includes self-help groups. This category includes cosmetic surgery providers, children's hospitals, but not sites of medical care for pets, which fall in Society and Lifestyle.
Medicine	Prescribed Medications: Sites that provide information about approved drugs and their medical use. Supplements and Unregulated Compounds: Sites that provide information about or promote the sale or use of chemicals not regulated by the FDA (such as naturally occurring compounds). This category includes sites of online shopping for medicine, as it is a sensitive category separated from regular shopping.

6. Responsibilities

6.1 Agencies that choose to seek an exemption for categories identified in Section 4 that require the Service Request process, shall follow the procedures outlined in the Service Request process document located at: https://itcentral.pa.gov/Pages/Enterprise-Services.aspx (CWOPA access only). For the Policy Waiver process, Agencies shall follow ITP-BUS004 *IT Waiver Review Process.*

6.2 Agency Information Security Officers (ISOs) or designates shall ensure agency internet traffic is in accordance with this policy.

6.3 Enterprise Chief Information Security Officer (EISO) will regularly audit entity filtering policies for compliance with this policy and its associated standards.

6.4 Third-party vendors, licensors, contractors, or suppliers providing services to the Commonwealth must comply with the requirements outlined in this ITP and OPD-SEC000B *Security Policy Requirements for Third Party Vendors*.

7. 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-SEC000B – *Security Policy Requirements for Third Party Vendors*
- OPD-SEC003A *Enterprise URL Deny/Allow Rule Set (Authorized CWOPA personnel only.* Contact RA-ITCentral@pa.gov for information*)*
- ITP-BUS011 *Commonwealth Cloud Computing Services Requirements*

- ITP-SEC000 *Information Security Policy*
- ITP-SEC024 *IT Security Incident Reporting Policy*

8. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9. 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 are to be directed to RA-ITCentral@pa.gov.

10. 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 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	01/18/2007	Base Document	N/A
Revision	08/30/2012	Standard Refresh	N/A
Revision	04/02/2014	ITP Reformat; Merged OPD-SEC003B, STD-SEC003A into ITP	N/A
Revision	10/29/2014	Updated COPPAR acronym	N/A
Revision	05/07/2015	In Section 6, added language/mandatory exception table requiring agencies to allow unrestricted access to a number of URLs	N/A
Revision	01/06/2016	In Section 6, added language/mandatory exception table requiring agencies to allow unrestricted access to a number of URLs	N/A
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	N/A
Revision	03/19/2018	Added OPD-SEC003A Enterprise URL Deny/Allow Rule Set Revised Enterprise Minimum Blocking Configuration Table Removed Retire Product table	N/A
Revision	06/03/2019	Removed Contain/Retire tables Replaced "COPPAR" with "Policy Waiver" in configuration table's Exemption Process fields Added additional categories for enterprise blocking	Revised IT Policy Redline <06/03/2019>
Revision	04/14/2020	Added outbound internet traffic guidance	Revised IT Policy Redline <04/15/2020>

Revision	07/12/2021	• Added offices under Scope • Added language for Third Party Vendors • Revised Block section per OPD-SEC003A • Amended name of ITP	Revised IT Policy Redline <07/12/2021>