pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

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

ITP Number ITP-SEC003	***Effective Date*** August 8, 2012
Category Recommended Policy	***Supersedes***
Contact RA-ITCentral@pa.gov	***Scheduled Review*** Annual

This Information Technology Policy (ITP) establishes standard policies for use of the commonwealth's Internet access control and content filtering (IACCF) solution for controlling and filtering internet traffic.

1. Purpose

Spyware, adware, viruses, phishing attacks and other malicious code have the potential to impair performance, increase costs and expose sensitive data to unauthorized parties. In order to protect the commonwealth network and IT resources from Internet threats, the Office of Administration issues the following policy on the use of an Internet access control and content filtering solution. This solution will allow 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 CoPA 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	Technology Classification
Current Telecom Service/Product Offerings	Current Telecom Service/Product Offerings	Web Filtering Solution	Current

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	Technology Classification

RETIRE

(These technologies are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.)

Technology	Platforms	Category	Technology Classification
SurfControl Web Filter	Microsoft Windows	Web Filtering Solution	Contain
SurfControl Web Filter	Microsoft ISA	Web Filtering Solution	Contain
WebSense Enterprise	Microsoft, Check Point, Cisco Systems, Juniper Networks and Network Appliance	Web Filtering Solution	Contain
WebMarshall			
Web Inspector			

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards.
At the present time, 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	Technology Classification
--	--	--	

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:

Enterprise minimum blocking configuration:

Category	Description
Child Pornography	Sites that include a visual or text depiction of a minor engaging in sexually explicit conduct.
File Storage/Sharing	Sites that provide secure, encrypted, off-site backup and restoration of data. These online repositories are typically used to store, organize and share videos, music, movies, photos, documents, and other electronically formatted information. Sites that fit these criteria essentially act as your hard drive on the Internet.
Malicious Outbound Data/Botnets	Sites to which botnets or other malware (as defined in the Malicious Sources category) send data or from which they receive command-and-control instructions. Includes sites that contain serious privacy issues, such as “phone home” sites to which software can connect and send user information. Usually does not include sites that can be categorized as Malicious Sources.

Category	Description
Malicious Sources/Malnets	Sites that host or distribute malware or whose purpose for existence is as part of the malware ecosystem. Malware is defined as software that takes control of a computer, modifies computer settings, or collects or reports personal information without the permission of the end user. It also includes software that misrepresents itself by tricking users to download or install it or to enter personal information. This includes sites or software that perform drive by downloads; browser hijackers; dialers; any program that modifies your browser homepage, bookmarks, or security settings; and key loggers. It also includes any software that bundles malware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as email addresses, name, social security number, IP address, etc. A site is not classified as malware if the user is reasonably notified that the software will perform these actions (e.g., it alerts that it will send personal information, be installed, or that it will log keystrokes).
Hacking	Sites that distribute, promote, or provide hacking tools and/or information which may help gain unauthorized access to computer systems and/or computerized communication systems. Hacking encompasses instructions on illegal or questionable tactics, such as creating viruses, distributing cracked or pirated software, or distributing other protected intellectual property.
Adult/Mature Content	Sites that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These sites include very profane or vulgar content and sites that are not appropriate for children.
Peer-to-Peer (P2P)	Sites that distribute software to facilitate the direct exchange of files between users. P2P includes software that enables file search and sharing across a network without dependence on a central server.
Personals/Dating	Sites that promote interpersonal relationships.
Phishing	Sites that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (e.g., credit card numbers, PIN numbers).
Pornography	Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Proxy Avoidance	Sites that provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server. This category includes any service which will allow a person to bypass the Blue Coat filtering system, such as anonymous surfing services.

Category	Description
Remote Access Tools	Sites that primarily focus on providing information about and/or methods that enable authorized remote access to and use of a desktop computer or private network.
Spam	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.
Streaming Internet Television, Radio, or Movie Applications	Internet Applications associated with providing paid or unpaid streaming television, radio, or movie content.
URL (Link) Shortening Services	Internet services that generate shortened URL's and redirect the user to the original longer URL's

Agencies shall make the following exception to allow access to the following: **http://www.facebook.com**

No "allow" rules may appear before this rule without a waiver request submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process.

Agencies may create any amount of more restrictive rules per their business requirements.

7. Responsibilities

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

Agency Information Security Officers (ISO's) or designates are to ensure are to ensure agency internet traffic is in accordance with this policy.

8. Related ITPs/Other References

- None

9. Authority

- Executive Order 2011-05, 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.

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

Version	Date	Purpose of Revision
Original	1/18/2007	Base Document
	8/30/2012	Standard Refresh
	4/2/2014	ITP Reformat; Merged OPD-SEC003B, STD-SEC003A into ITP
	10/29/2014	Updated COPPAR acronym