COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **Network Security Policy**	Number: **POL-SEC007**
Domain: **Security**	Category:
Date Issued: **06/20/11**	Issued By Direction Of:
Date Revised: **10/11/2013**	 Sandra Patterson, CIO Bureau of Information Systems

Table of Contents

Document History

Version	Date	Author	Status	Notes
1.0	06/20/2011	David Johnson	Draft	Initial creation
2.0	06/23/2011	David Johnson	Revision	Revised per Tom Zarb Review
3.0	10/11/2013	Bob Myers	Revision	Revised to reflect current standards and architecture

1 Introduction

1.1 Purpose

This policy establishes requirements to protecting data in transit for Department of Public Welfare (DPW) information systems. Requirements include compartmentalizing security functionalities; maintaining the confidentiality, integrity, and availability of transmitted data; utilizing trusted sources to establish a communication path; and maintaining the integrity and availability of DPW systems and services. This policy also provides direction to ensure that applicable Commonwealth of Pennsylvania (CoPA) and federal requirements are followed.

1.2 Scope

All DPW employees, contractors and business partners are responsible for understanding and complying with this policy.

1.3 Compliance

Violations of this policy may lead to revocation of system privileges and/or disciplinary action.

1.4 Exemptions

Requests for exemption to the policy should be submitted to the Chief Information Security Officer (CISO). Any exceptions granted will be issued a policy waiver for a defined period of time.

1.5 Policy Review and Update

This document, and its supporting standards and procedures, will be reviewed annually, and updated as needed.

2 Information Flow Enforcement

Information flow enforcement relates to the protection of the confidentiality, integrity, and availability of DPW information systems and DPW information as it flows between networks. The control family ensures the establishment of an effective physical and logical network security perimeter and provides guidance for best protecting information as it moves both within the security perimeter and as it moves to and from other networks outside the security perimeter such as the Internet.

2.1 Boundary Protection

Within DPW, boundary protection of information technology resources is accomplished by the installation and operation of controlled interfaces (e.g., proxies, gateways, routers, firewall, and encrypted tunnels). Controlled interfaces track and control data, encrypt data and determine whether to pass or drop data.

DPW Policy

Interconnections

a. The DPW network security administrator shall ensure that all connections to the Internet and other external networks or information systems are authorized, encrypted, documented and occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels).
b. The DPW network security administrator shall minimize the number of access points to agency information systems, for better monitoring of inbound and outbound network traffic.
c. The DPW network security administrator shall implement firewall and intrusion detection/ prevention technologies at the edge of DPW's network, including the Internet Gateway, to protect sensitive internal information assets from unauthorized access.

DPW Policy

d. The DPW network security administrator shall establish, maintain and review at least annually, traffic flow policies (on firewalls and intrusion prevention systems) for each managed interface.

e. The DPW network security administrator shall ensure that, as applicable, Web-enabled applications, and other services provided through the Internet, are deployed on a Demilitarized Zone (DMZ) or proxied from the DMZ.

f. The DPW network security administrator shall maintain agency firewalls per CoPA policy, provided in ITB-SEC011, *Enterprise Policy and Software Standards for Agency Firewalls*, and ITB-SEC034, *Enterprise Firewall Rule Set*. The DPW network security administrator shall implement firewalls for the protection of CoPA web applications per CoPA policy, provided in ITB-SEC004, *Enterprise Web Application Firewall.*

g. The DPW network security administrator shall maintain the agency's proxy server policy in accordance with Commonwealth of Pennsylvania (CoPA) policy, provided in ITB-SEC003, *Enterprise Security Auditing and Monitoring - Internet Access Control and Content Filtering (IACCF) Standard*.

h. Interconnections shall be encrypted per DPW's *Cryptography Policy*.

Least Functionality

i. The DPW network security administrator shall configure the agency's boundary protection devices to provide only essential ports, protocols, and/or services in the network equipment, servers, storage and systems software to create a white-list of allowed items or that serve the agency's particular purpose.

Default Denial

j. The DPW network security administrator shall configure boundary protection devices to block every network connectivity path and network service not explicitly authorized by the CISO.

Configuration Changes and Documentation

k. All changes to firewall configuration parameters, enabled services, and permitted connectivity shall be authorized by the CISO, and documented in accordance with change control policies and procedures.

l. Privileges to modify the functionality, connectivity, configuration and services supported by network perimeter devices, including firewalls and intrusion detection/prevention systems, shall be restricted to the CISO and personnel specifically authorized by the CISO.

Audit Logging and Monitoring

m. System owners and the DPW network security administrator shall ensure that the audit logs for each network security system meet the requirements of DPW's *Security Audit Logging Policy*.

Periodic Review

n. The DPW network security administrator shall periodically review firewall configurations, to ensure their effectiveness and compliance with agency and CoPA security policies. Documentation shall be maintained that: (1) identifies the CISO-approved ports and services, (2) documents the results of periodic reviews, and (3) provides documented assurance that enabled ports and services conform to the CISO-approved configuration.

Vulnerability Scanning

o. System owners shall perform periodic vulnerability scanning to meet the DPW standard, STD-ENSS020 (Web Application Security Scanning Standard) and CoPA policies, ITB-SEC005 (Commonwealth Application Certification and Accreditation) and ITB SEC023 – Security Assessment and Testing Policy).

2.2 Remote Access

Remote access controls restrict authorized remote access (e.g., using virtual private network (VPN) technology) and protect against unauthorized connections or subversion of authorized connections. Remote access controls apply to information systems other than public web servers or systems

specifically designed for public access. The following policy provides guidance for the implementation and monitoring of remote access capabilities.

DPW Policy

a. DPW network security administration or the program office shall authorize the users requiring remote access, including remote access for privileged functions, and shall document the rationale for such access.

b. The DPW network security administrator shall ensure that:
   - remote access is controlled through a limited number of managed access control points;
   - automated mechanisms are employed to facilitate the monitoring and control of remote access sessions; and
   - remote access for privileged functions shall be used (e.g., maintenance ports and system and device administration) only for compelling operational needs.

c. Remote access shall be limited to official use by individuals authorized by DPW management to work at home, or other non-DPW worksite,

d. DPW employees, business partners and contractors, while remotely accessing DPW information and/or information systems shall not:
   - Copy DPW-related documents to the hard drives of personally- or privately-owned computers; or
   - Use unapproved peer-to-peer file-sharing software (e.g., LimeWire, Napster).

2.3 Wireless Access

Wireless communications technologies include the following:

- Wireless systems (e.g., wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN), peer-to-peer wireless networks, information technology systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols.

Wireless Access Points are inherently insecure. The following policy provides a guidance to ensure that any use of wireless technologies is protected from compromise.

DPW Policy

Wireless Access

The DPW network security administrator shall ensure, at a minimum the following:

- Encryption protection is enabled for wireless access
- MAC address authentication is utilized
- Static IP addresses, not DHCP, is utilized
- Personal firewalls are utilized on wireless clients
- File sharing is disabled on wireless clients
- Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.
- Intrusion detection agents are deployed on the wireless side of the firewall; and
- A firewall is implemented between the wireless network and the wired infrastructure;

Wireless Access Point Restrictions

a. As defined in DPW's *Data Encryption Standards*, general DPW policy prohibits use of Wireless Access Point (WAP) devices. Any exceptions to this policy must be approved by the CISO and must comply with ITB-NET001- *Wireless LAN Technology*, and other applicable DPW and CoPA policy.

b. Wireless Access Point identifier broadcasting (SSIDs) shall be set to "Disabled" by default and shut down when not in use (i.e., nights, weekends).

c. The DPW network security administrator shall periodically (quarterly) scan for unauthorized wireless points and take appropriate action if such access points are discovered.

3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software provides the ability to create virtual machines that reduce the amount of hardware needed. Use of partitioning and virtualization technologies requires consideration of related security considerations.

3.1 Partitioning

Information system partitioning, including separation of user functionality from system management functionality, is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. System Owners should implement controls that assure the partitioning of information system components and domains if disparities in the security categorization of system components and the size and volume of transactions at the disparate security levels would be better served by such partitioning.

DPW Policy

a. The CISO shall ensure that DPW applications, services, or information systems physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

b. The DPW network security administrator shall ensure that all enterprise network architectures operated by, or on behalf of, DPW are designed to support, at a minimum, separate public, “demilitarized” and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones shall be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by the CISO.

3.2 Security Function Isolation

The following policy provides guidance to ensure that DPW information systems are capable of separating security functions from non-security functions.

DPW Policy

a. Program Offices and System Owners shall ensure that information system security functions are implemented and maintained independent from the system.

3.3 Virtualization Techniques

Virtualization, a method of dividing the resources of a computer (hardware and software) into multiple execution environments, presents unique security considerations that must be addressed.

DPW Policy

a. CoPA policy governing server virtualization is provided in ITB-SYM008, Server Virtualization Policy.

b. Program Offices/System Owners shall ensure that the following controls are implemented in a virtual environment:

- The host is isolated from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
- Audit logs for all virtual machines and hosts are generated, and stored outside the virtual environment.

DPW Policy

- Virtual Machines that are Internet facing (web servers, portal servers, etc.) are physically separated from Virtual Machines that process internally.
- Device drivers that are “critical” are physically separated.

4 Appendix

4.1 References

Document	Type
Data Encryption Standards	DPW Policy
Network Security Requests	DPW Policy
Outbound Internet Proxy and Content Filtering	DPW Policy
Web Applications Security Scanning	DPW Policy
ITB-NET001- Wireless LAN Technology	CoPA ITB
ITB-SEC003 - Enterprise Security Auditing and Monitoring - Internet Access Control and Content Filtering (IACCF)	CoPA ITB
ITB-SEC004 - Enterprise Web Application Firewall	CoPA ITB
ITB-NET005 - Commonwealth External and Internal Domain Name Services (DNS)	CoPA ITB
ITB-SEC010 - Virtual Private Network Standards	CoPA ITB
ITB-SEC011 - Enterprise Policy and Software Standards for Agency Firewalls	CoPA ITB
ITB-SEC034 - Enterprise Firewall Rule Set	CoPA ITB
ITB-SYM008 - Server Virtualization Policy	CoPA ITB