COMMONWEALTH OF PENNSYLVANIA DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **System and Information Integrity Policy**	Number: **POL-SEC011**
Domain: **Security**	Category:
Date Issued: **06/22/11**	Issued By Direction Of: Sandra K. Patterson Sandra K. Patterson, CIO Bureau of Information Systems
Date Revised: **07/25/13**	

Table of Contents

1 Introduction

1.1 Purpose

This policy establishes requirements for protecting the integrity of DPW information and information systems. Safeguards include patching vulnerable software, malicious code prevention, data integrity protections and data input and output restrictions. Additionally, this policy 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 shall 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 Systems and Data Integrity

The following policy establishes requirements for protecting the integrity of DPW information systems and data.

DPW Policy

Patch Management

a. System owners shall maintain current, the system patch level, service packs and hot fixes. Host Security

b. System owners shall implement host security software for the information systems to meet the requirements of DPW standard, Enterprise Host Security Suite Software Standards (STD-ENSS024) and the CoPA policy, Enterprise Host Security Software Suite Standards and Policy (ITB-SEC001).

Software and Data Integrity

c. Program Offices and System Owners shall ensure that information systems prevent and detect unauthorized changes to software and data.

d. DPW shall employ centrally managed automated tools to identify and notify modifications to system integrity.

Network Disconnect

e. The DPW network security administrator shall ensure that DPW applications are configured to terminate network connections at the end of a session or after twenty minutes of inactivity.

Denial of Service Protection

f. The DPW network security administrator shall ensure that DPW information systems are configured to protect against the effects of denial of service attacks

Mobile Code

DPW Policy
g. DPW employees or contractors shall not download, install and use mobile code (such as ActiveX or JavaScript) that has not been approved by the CISO. **Fail in a Known Secure State** h. System Owners shall ensure DPW information systems fail in a secure manner that preserves log data, last-user-logged-in data, and connectivity information; as well as ensure the confidentiality, integrity, and availability of the information resources. **Error Handling** i. System Owners shall ensure that DPW information systems are configured to identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries. **Security Functionality Verification** j. DPW information systems shall verify the correct operation of security functions upon system startup and restart. k. DPW shall employ automated mechanisms to: (1) support management of distributed security testing, and (2) provide notification of failed automated security tests. **Information Input Restrictions** l. DPW information systems shall allow input only from authorized personnel. m. DPW information systems shall check information inputs for accuracy, completeness, validity and authenticity. **Information Output Handling** n. Output from DPW information systems, both paper and digital, shall be accessed only by authorized personnel, protected from improper modification and disclosure, either accidental or malicious.

3 Appendix

3.1 References

Document	Type
An Introduction to DPW Computers	DPW Policy
DPW Enterprise Host Security Suite Software Standards (STD-ENSS024)	DPW Policy
DPW Internet Policy	DPW Policy
ITB-SEC001 - Enterprise Host Security Suite Software Standards	CoPA ITB
ITB-SEC002 - Internet Accessible Proxy Servers and Services	CoPA ITB

Policy Revision Log:

Change Date	Version	Change Description	Author and Organization
06/20/2011	1.0	Initial Creation	David Johnson
06/23/2011	2.0	Revised per Tom Zarb review	David Johnson
07/30/2013	2.1	Updated per Mathieu Saury review	Mathieu Saury