# COMMONWEALTH OF PENNSYLVANIA

# HEALTH & HUMAN SERVICES DELIVERY CENTER

# INFORMATION TECHNOLOGY PROCEDURE

|  |  |
| --- | --- |
| Name of Procedure: | Number: |
| **System and Information Integrity** | **PRO-SEC040** |
| Domain: | Category: |
| **Security** | **System** |
| Date Issued: | Issued by Direction Of: |
| **02/10/2021** |  |
| Date Revised: | **John Miknich, Chief** **Information Security Officer** |
| **02/10/2021** | **Health & Human Services Delivery Center** |

**Abstract:**

This policy establishes requirements for protecting the integrity of the Department of Human Services (DHS) 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.

**General:**

**Scope**

All DHS employees, contractors and business partners are responsible for understanding and complying with this procedure.

**Compliance**

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

**Procedure:**

# System and Information Integrity

System Integrity Policy: DHS's Information Security Policy and Standards, in addition to the guidance provided by the Commonwealth Governor’s Office of Administration, provide foundation based on NIST SP 800-53 rev 4. DHS has established a formal, documented System and Information Integrity Policy (POL-SEC011) that has a stated purpose as below:

*“The policy establishes requirements for protecting the integrity of DHS 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.”*

The other relevant DHS and Commonwealth IT security policies and standards include

* DHS policy POL-SEC011 – DHS Cryptography policy
* DHS standard STD-ENSS024 – DHS Enterprise Host Security Suite Software Standards
* DHS Internet Policy
* Commonwealth ITP-SEC001 – Enterprise Host Security Suite Standards
* Commonwealth ITP-SEC002 – Internet Accessible Proxy Servers and Services
* Commonwealth ITP-SEC003 - Enterprise Security Auditing and Monitoring-Internet Access Control and Content Filtering Standard

b. System Integrity Procedures: The above identified policies and standards addresses the roles, commitment and coordination related to the following elements of integrity:

* Patch Management
* Host Security
* Software and Data Integrity
* Network Disconnect
* Denial of Service Protection
* Mobile Code
* Fail in a known secure state
* Error Handling
* Security Functionality Verification
* Information Input Restrictions and

Information Output Handling.

# Exemptions

Requests for exemption to the procedure 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.

# 

**Refresh Schedule:**

All procedures and referenced documentation identified in this document will be subject to review annually and updated as needed or upon request by the HHS Delivery Center Domain Leads.

**Procedure Revision Log:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Change Date** | **Version** | **Change Description** | **Author and Organization** |
| 02/10/2021 | 1.0 | Document Creation | John Miknich |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |