# COMMONWEALTH OF PENNSYLVANIA

#  HEALTH & HUMAN SERVICES DELIVERY CENTER

# INFORMATION TECHNOLOGY PROCEDURE

|  |  |
| --- | --- |
| Name of Procedure: | Number: |
| **Security Assessment and Authorization**  | **PRO-SEC037** |
| Domain: | Category: |
| **Security** | **Assessment** |
| 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:**

The purpose of this directive is to establish a Security Assessment and Authorization Procedure to provide actions and decisions to facilitate the Security Assessment and Authorization policies and related security controls, including responsibilities, requirements and principles for the applicable processes to support Information Technology Management across the Department of Human Services (DHS).

**General:**

Security Assessment and Authorization Procedures address the effective implementation of selected security controls and control enhancements in the Security Assessment and Authorization control family. The Security Assessment and Authorization Procedure at DHS is intended to detail the effective implementation of the processes necessary to meet the Security Assessment and Authorization requirements of Federal and Pennsylvania state laws, regulations, and leading information security practices (e.g., National Institute of Standards and Technology [NIST] Special Publication 800-53 Revision 4 & the Internal Revenue Service [IRS] Publication 1075).

**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:**

| **DHS Procedure** |
| --- |
| 1. DHS shall meet or exceed all Federal regulatory policies and procedures which affect Security Assessment and Authorization processes to be implemented on DHS information technology assets. This includes the following procedures:

Security Assessments1. DHS has established and operationalized STD-ENSS031: Risk Management Standard that shall be used to help perform periodic risk assessments on the department’s IT infrastructure. Health & Human Services Delivery Center (HHS DC) Information Security Office (ISO) Security Architecture Section shall conduct an assessment of the security controls in the information system to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
2. DHS shall develop a security assessment plan that describes the scope of the assessment, including:
3. Controls and control enhancements under assessment.
4. Procedures to be used to determine control effectiveness.
5. Environment, assessment team, and assessment roles and responsibilities.
6. DHS shall ensure that the assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the security assessment.
7. DHS shall assess the controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.
8. DHS shall produce a security assessment report that documents the results of the assessment.
9. DHS shall provide the results of the security control assessment to HHS DC ISO Chief Information Security Officer (CISO) who shall review the gaps identified in the assessment and establish a corrective action plan with the appropriate stakeholders.

**System Interconnections**1. DHS shall protect and monitor information system interconnections by performing the following activities:
	* 1. Extend the existing memorandum of understanding and Business Associate Agreement with Commonwealth agencies and external entities accessing applicable web applications. Users shall sign and abide by the Commonwealth’s Management Directive 205.34: Acceptable Use of IT Resources.
		2. Document system connections, interface characteristics, security requirements, and the nature of the information communicated.
		3. Use the boundary protection solutions to help monitor connections established on the information systems supporting interconnections. Collect and generate logs to review performance of security controls.

**Plan of Actions and Milestones**1. DHS shall develop, update, and periodically review a Plan of Actions and Milestones (POA&M) that details deficiencies identified during security control assessments or continuous monitoring activities, and documents the planned remedial actions of the agency to correct weaknesses in order to reduce or eliminate known vulnerabilities in the system.

**Security Authorization**1. DHS shall assign an authorizing official for the system and for any common controls inherited by the system, and ensure the official completes the following before commencing operations:
	* 1. Authorizes the system for processing
		2. Authorizes the common controls inherited by the system
2. DHS shall follow the Commonwealth Application Certification and Accreditation (CA)2 policy (ITP-SEC005), which states the Commonwealth’s web applications are to undergo the reaccreditation process on a triennial basis.

**Continuous Monitoring**1. DHS shall develop a security continuous monitoring strategy and program, and establish the following mechanisms:
	* 1. A configuration management process for the information system and its constituent components.
		2. A determination of the security impact of changes to the information system and environment of operation.
		3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.
		4. Reporting the security state of the information system to appropriate organizational officials within 365 days.
 |

**Appendix:**

|  |  |
| --- | --- |
| Document | Type |
| National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4) | Federal Standard |
| IRS Publication 1075 | Federal Guidance |
| CMS Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E) Version 2.0 | Federal Guidance  |
| Management Directive (MD) 205.34: Acceptable Use of Commonwealth IT Resources | COPA MD |
| STD-ENSS031: Risk Management Standard | DHS Standard |
| ITP-SEC005: Commonwealth Application Certification and Accreditation | COPA Policy |

**Exemptions:**

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

**Refresh Schedule:**

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

**Procedure Revision Log:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Change Date** | **Version** | **Change Description** | **Author and Organization** |
| 12/9/2020 | 1.2 | Update content | Kyle Valeski - Deloitte |
| 2/10/2021 | 1.2 | Format changes | P. Gillingham |
|  |  |  |  |
|  |  |  |  |