#  COMMONWEALTH OF PENNSYLVANIA

#  HEALTH & HUMAN SERVICES DELIVERY CENTER

# INFORMATION TECHNOLOGY PROCEDURE

|  |  |
| --- | --- |
| Name of Procedure:  | Number: |
| **Security Planning** | **PRO-SEC038** |
| Domain: | Category: |
| **Security** | **Planning** |
| Date Issued:  | Issued by Direction Of: |
| **02/10/2021** |  |
| Date Revised: **02/10/2021** | **John Miknich, Chief Information Security Officer** **Health & Human Services Delivery Center** |

**Abstract:**

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

**General:**

As systems have increasingly taken on a strategic role at DHS, proper planning can provide a security level commensurate with the risk associated with the operation of those systems. Having security controls in place, such as the development of a System Security Plan, can provide an overview of the security requirements of the system and how the security controls meet those requirements. Security Planning Procedures address the effective implementation of selected security controls and control enhancements in the planning control family. The Security Planning Procedure at DHS is intended to detail the effective implementation of the processes necessary to meet the Security Planning 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).

**Procedure:**

**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.

# Security Planning Procedure

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

System Security Plan1. Security Architecture Section shall develop and maintain the System Security Plan (SSP). The SSP shall:
	* 1. Be consistent with the agency’s safeguarding requirements.
		2. Explicitly define the information systems that receive, process, store, or transmit sensitive information.
		3. Describe the operational context of the information system in terms of missions and business processes.
		4. Describe the operational environment for the information system and relationships with or connections to other information systems.
		5. Provide an overview of the security requirements for the system.
		6. Include any relevant overlays, if applicable.
		7. Document the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions.
		8. Be reviewed and approved by the authorizing official or designated representative prior to plan implementation.
2. Security Architecture Section shall distribute copies of the SSP and communicate subsequent changes to designated agency officials and Federal offices.
3. Security Architecture Section shall review the SSP on an annual basis.
4. Security Architecture Section shall update the SSP to address changes in the information system/environment of operation or problems identified during plan implementation or security control assessments.
5. Security Architecture Section shall protect the SSP from unauthorized disclosure and modification.

**Plan/Coordinate with Other Organizational Entities**1. DHS shall take measures to communicate the security-related activities to the relevant stakeholders of the information system before conducting such activities to reduce the impact on other organizational entities.

**Rules of Behavior** 1. DHS shall maintain rules of behavior for accessing sensitive data and/or using information systems containing sensitive data, as established in Management Directive (MD) 205.34: Acceptable Use of Commonwealth IT Resources that outlines acceptable use behavior with regards to Commonwealth data, information system, and use of networks.

**Social Media and Networking Restrictions**1. DHS shall include in the rules of behavior explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. DHS shall follow the guidelines established in Management Directive 205.42: Social Media and Management Directive 205.34: Acceptable Use of Commonwealth IT Resources.
 |

**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 |
| Management Directive (MD) 205.42: Social Media | COPA MD |

# 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.

**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** |
| 02/10/2021 | 1.0 | Initial | J. Miknich |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |