# COMMONWEALTH OF PENNSYLVANIA

# HEALTH & HUMAN SERVICES DELIVERY CENTER

# INFORMATION TECHNOLOGY PROCEDURE

|  |  |
| --- | --- |
| Name of Procedure: | Number: |
| **System and Communication Protection** | **PRO-SEC039** |
| Domain: | Category: |
| **Security** | **System** |
| Date Issued: | Issued by Direction Of: |
| **01/07/2021** |  |
| Date Revised: | **John Miknich, Chief Information Security Officer** |
| **4/06/2021** | **Health & Human Services Delivery Center** |

**Abstract:**

The purpose of this directive is to establish System and Communication Protection procedures to provide actions and decisions to be performed to accomplish the requirements identified in the System and Communication Protection Policy, including responsibilities, requirements and principles for System and Communication Protection processes to support Information Technology Management across the Department of Human Services (DHS).

**General:**

System and communications protection controls provide safeguards for the system to address the confidentiality and integrity of information at rest and in transit, through physical or logical means. The System and Communication Protection Procedure at DHS is intended to detail the effective implementation of the processes necessary to meet the system and communication protection 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 and 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:**

# System and Communication Protection Procedure

| **DHS Procedure** |
| --- |
| 1. DHS meets or exceeds all Federal regulatory policies and procedures which affect system and communication protection processes to be implemented on DHS information technology assets through the following procedures:  Application Partitioning  1. DHS separates user functionality (including user interface services) from information system management functionality by adhering to the guidelines for application partitioning in POL-SEC007: Network Security Policy.    * 1. The Health & Human Services Deliver Center (HHS DC) Chief Information Security Officer (CISO) ensures that DHS applications, services, or information systems physically or logically separate user interface services from information storage or management services. 2. DHS follows a three-tier approach to implementing web applications that includes the application tier, the business tier, and the data tier, with each layer being maintained using logical and/or physical partitioning:    * 1. The application tier (user interface) resides on the webserver that is protected within the DHS DMZ and the DHS boundary protection solutions.      2. The business tier (underlying system rules) is maintained using the Corticon Business Rules Engine Solution and will be maintained separate from the application tier. Middleware solutions serves as the means of transport between the two tiers.      3. The data tier (data at rest) is logically accessible using database user roles. The database server resides on a separate information system.  Information in Shared System Resources  1. For applications handling sensitive data, DHS uses shared resources through an object re-use mechanism provided by a standard Microsoft .NET framework, which flushes/deletes the object data prior to reuse to prevent unauthorized and unintended information transfer via shared system resources. Access is also be controlled to these resources through role-based access control, as detailed in POL-SEC012: User Identity and Access Management, with access to DHS IT Infrastructure being based on Commonwealth user credentials and assigned user groups.   **Denial of Service Protection**   1. HHS DC Information Security Office (ISO) Security Architecture Section along with the Commonwealth datacenter have established and manage a defense in depth boundary protection solution that helps prevent/limit the impacts from Denial of Service attacks, which includes the following defenses:    * 1. Use of De-Militarized Zones to protect the server infrastructure.      2. CISCO IronPort to protect against email spams.      3. HHS DC ISO’s CheckPoint Firewall, Commonwealth’s ~~Blue Coat~~ Fortinet web proxy/firewall and the McAfee network IPS at the network level.      4. Microsoft ISA and Imperva Web application firewall at the web application level.      5. McAfee antivirus to protect at the system level.      6. Windows event log monitoring using Microsoft SCOM (24x7 monitoring at the datacenter) to detect events at the system level.   **Boundary Protection**   1. HHS DC ISO Security Architecture Section along with the Commonwealth datacenter protect the network boundary hosting sensitive information through the following controls:    * 1. Manage the firewall and intrusion detection/prevention technologies that have been implemented at the DHS network boundary, including the Internet Gateway, to protect sensitive internal information assets from unauthorized access. The agency will adhere to the Commonwealth ITP-SEC011: Enterprise Policy and Software Standards for Agency Firewalls to help ensure the security of information technology assets and to allow the Commonwealth to meet and fully comply with federal regulations.      2. To implement a secure managed interface for each external telecommunication service, DHS adheres to the Commonwealth ITP-NET003: Enterprise Telecommunications Contracts and the Commonwealth’s Office of Administration who manages the telecommunication services that DHS consumes.      3. DHS adheres to Commonwealth ITP-SEC011: Enterprise Policy and Software Standards for Agency Firewalls and ITP-SEC034: Enterprise Firewall Rule Set for the establishment of traffic flow for each managed interface.      4. Communication between web and database servers or web and end-user is performed by using one or both of the following means: PKI or Entrust certificates and ciphers and protocols from within the operating system. DHS conforms to current security standards by deprecating older and unused ciphers and protocols as identified by either the Office of Administration and/or the Internal Revenue Service(IRS) and their periodic audit of DHS computer systems. Local PKI certificates or those obtained through Entrust adhere to the proper and current security algorithms as again defined by the Office of Administration and/or the IRS and their periodic audit of DHS computer systems.      5. HHS DC CISO is responsible to provide exceptions to the existing traffic flow policy on DHS’s managed interfaces, and to review the exceptions on an as-needed basis. The request is documented and maintained to meet the department’s PRO-ENSS017: Network Security Requests procedure.      6. DHS follows the HHS change control process to perform changes to the DHS firewall. All requests are submitted using the Service Now application/tool. Standard Firewall rule changes are reviewed by the change control management team for approval. Other changes such as normal changes are approved by the Change Control Board on a weekly basis. Emergency changes are reviewed by the Change Manager and one Board member. Changes can be made on a daily basis or during an authorized change window depending on the nature of the change.      7. HHS DC Technology Services Office(TSO) Operations Optimization and Support uses static IP address for DHS information systems. This requires any system to have a pre-filled IP address and related connectivity details prior to being connected to the DHS network. If an unauthorized device is plugged in, the server and network administration team will detect a potential collusion to existing IP address assignments. This existing procedure is also leveraged for using portable devices such as laptops and PDAs on the DHS network. HHS DC TSO Operations Optimization and Support is responsible to review and authorize the information systems prior to being connected to the DHS network in addition to providing a static IP address to the approved information system.   **Transmission Confidentiality and Integrity**   1. DHS protects the confidentiality and integrity of transmitted information through the following procedures:    * 1. DHS adheres to Commonwealth ITP-SEC031: Encryption Standards for Data in Transit for the protection of transmitted information.      2. Applicable DHS web applications use SSL technology to protect the communication of data between the web server and the end-user’s browser. The integrity protection mechanisms include use of certificates to maintain integrity of the web application communication.   **Network Disconnect**   1. To address the termination of network connections that are associated with communication sessions, DHS applies the following controls:    * 1. HHS DC Technology Services Office(TSO) Network Division enables the use of Dynamic Host Configuration Protocol(DHCP) and the use of static IP addresses for infrastructure.   **Cryptographic Key Establishment and Management**   1. DHS uses Enterprise Data Exchanges web service. The cryptographic keys are maintained, monitored and managed using the following processes:    * 1. DHS adheres to the Commonwealth’s Public Key Infrastructure guidance that is established in ITP-SEC013, Identity Protection and Access Management Architectural Standard-Identity Management Services, and defined in GEN-SEC013G, the Commonwealth policy for Public Key Infrastructure certificates.   **Cryptographic Protection**   1. HHS DC ISO Security Architecture Section has established the DHS cryptography policy (POL-SEC002) based on applicable federal and Commonwealth regulations, policies and standards. Based on the guidelines established through POL-SEC002, DHS uses the following secure communication protocols:    * 1. Secure Sockets Layer (SSL) v3/Transport Layer Security (TLS)v1.2.      2. Secure Shell v2(SSH-2).      3. Secure File Transport Protocol (SFTP) using SSH-2.   **Collaborative Computing Devices**   1. DHS does not use collaborative computing devices.   **Mobile Code**   1. DHS regulates the use of mobile code throughout the environment through the following procedures:    * 1. HHS DC Architecture Review Board has established an Application Lifecycle Management (ALM) process that describes the application technology, framework and versions that can be used to develop and support maintenance of web applications and web services. The current version of the ALM approves use of WebTwain ActiveX control. eCIS web applications use JavaScript which is used to enhance user experience.      2. DHS applicable applications follow STD-ENSS034: Web Application Vulnerability Assessment Standard for vulnerability scanning standards. The web applications are assessed for security vulnerabilities within the lower test phases prior to deployment to production environment. Java applets are required to be signed and approved by the department before use.      3. DHS applicable applications maintain their source code using Microsoft TFS including the mobile code used within the application. BIS Division of Enterprise Applications is responsible to maintain and manage access to the web application source code.   **Voice Over Internet Protocol**   1. DHS has established usage restrictions and implementation guidance for VoIP technologies:    * 1. DHS does not have sensitive PII, including FTI, on VoIP traffic.      2. VoIP network hardware (including servers, routers, switches, and firewalls) is physically protected in accordance with the minimum protection standards for physical security as outlined in Section 4.0 of IRS Publication 1075. DHS adheres to the guidelines defined by the POL-SEC008: Physical and Environmental Security Policy in order to properly safeguard and monitor the security of system components at the Willow Oak Building and both the primary and alternative data centers. 2. DHS authorizes, monitors, and controls the use of VoIP within the information system through the following procedures:    * 1. All calls across the VoIP network are encrypted. DHS has implemented VoIP encryption on the entire VoIP platform, encrypting signaling messages between end points.      2. The Commonwealth has implemented encryption software on all VoIP cluster servers and rolled out encryption certificates to endpoint phones. DHS adheres to Commonwealth ITP-NET002: Network Router and Switch Technology Standards.   **Session Authenticity**   1. HHS DC Technology Services Office(TSO) Network Division and HHS DC ISO Security Architecture Section provide the following mechanisms to protect the authenticity of communications sessions.:    * 1. DHS IAM solution (CA SiteMinder) session is maintained based on user authentication and authorization to the applicable web applications. The CA SiteMinder session is maintained as an encrypted cookie value within the HTTP header and is maintained unique for each user session. The session cookie is flushed once a user log out operation is detected in the applicable web applications. Upon a session timeout, the user is challenged to provide their user credentials. For session management, DHS adheres to POL-SEC012: User Access and Identity Management. For further SiteMinder procedures, DHS adheres to PRO-ENSS024: SiteMinder Archiving.      2. The applicable web applications use standard Microsoft .NET framework session ID. This session ID is maintained unique for each user session.      3. *For Virtual Private Network (VPN) sessions, DHS relies upon the Enterprise managed Cisco AnyConnect Secure Mobility Client. Upon a session timeout, the user is challenged to provide their user credentials*   **Protection of Information at Rest**   1. DHS protects the confidentiality and integrity of data at rest as identified in ITP-SEC020: Encryption Standards for Data at Rest, and by employing the following safeguards:    * 1. HHS DC TSO Operations Database Division maintains appropriate role-based access controls for access to applicable web application data. The access to data is restricted to database administrators only. In addition, the web application databases are configured to maintain a log of data control language operations that are used to control access to data stored in a database.      2. DHS web applications use Role Based Access Control framework operationalized using DHS IAM solutions. The DHS IAM solutions provide authentication and authorization functions to web pages/web services and data accessed, as referenced in POL-SEC012: User Access and Identity Management. In addition, applicable web applications maintain a workflow log that contains a record of user actions (create, modify and delete) performed on benefit eligibility cases.      3. The agency ensures the physical security by adhering to POL-SEC008: Physical and Environmental Security Policy. DHS ensures the security of the Commonwealth datacenter by ensuring the facility has state-of-the-art access controls in place, including no public access, multifactor identification, multi-level security zones, cameras, etc. |

**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 |
| POL-SEC002: Cryptography Policy | DHS Policy |
| POL-SEC007: Network Security Policy | DHS Policy |
| ITP-SEC011: Enterprise Policy and Software Standards for Agency Firewalls | CoPA Policy |
| ITP-SEC020: Encryption Standards for Data at Rest | CoPA Policy |
| ITP-SEC013: Identity Protection and Access Management Architectural Standard-Identity Management Services | CoPA Standard |
| GEN-SEC013G: Commonwealth policy for Public Key Infrastructure certificates | CoPA Policy |
| PRO-ENSS017: Network Security Requests | DHS Procedure |
| ITP-SEC031: Encryption Standards for Data in Transit | CoPA Policy |
| ITP-SEC034: Enterprise Firewall Rule Set | CoPA Policy |
| STD-ENSS034: Web Application Vulnerability Assessment Standard | DHS Standard |
| POL-SEC012: User Access and Identity Management | DHS Policy |
| PRO-ENSS024: SiteMinder Archiving | DHS Procedure |
| STD-ENSS035: Remote Access Control | DHS Standard |
| ITP-SEC010: Virtual Private Network Standards | CoPA Policy |
| POL-SEC008: Physical and Environmental Security Policy | DHS Policy |

# 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** |
| 04/06/2021 | 1.0 | Document Creation | John Miknich |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |