	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1908 01/05/2022 01/05/2024

SUBJECT: DHS Information Security Policies

Personnel Security Policy

POLICY

This policy establishes the Enterprise Personnel Security Policy, for managing risks from personnel screening, termination, management and third-party access, through the establishment of an effective security planning program. The personnel security program helps DHS implement security best practices with regard to personnel screening, termination, transfer and management.

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services
4. Centers for Medicare & Medicaid Services
5. Georgia Technology Authority

References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, January 2015
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-18 “Guide for Developing Security Plans for Federal Information Systems” Revision 1 February 2006.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Managers” March 2007
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges

Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or

operated by DHS. Any information, not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Definitions

None

Responsibilities

DHS shall adopt the Personnel Security principles established in NIST SP 800-53 "Personnel Security," Control Family guidelines, as the official policy for this domain. The following subsections outline the Personnel Security standards that constitute DHS policy. Each DHS Business System is then bound to this policy, and shall develop or adhere to a program plan which demonstrates compliance with the policy related to the standards documented.

- **PS-1 Personnel Security Procedures**:
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing personnel security controls and preventing unauthorized access and use of agency IT resources and information systems on the basis of business and security requirements.
    2. Periodic reviews of this policy shall be performed and documented **at least within every three years**, or **when there is a significant change**.
    3. Periodic review of personnel security procedures shall be performed **at least annually**.
- **PS-2 Position Risk Designation**
    1. Assignment of a risk designation to all positions is completed by the DHS Human Resources Office.
    2. DHS adheres to the IRS Office of Safeguards minimum requirements for screening for individuals filling those positions.
    3. Position risk designations are reviewed and updated (as necessary) on an **annual** basis.
- **PS-3 Personnel Screening**
    1. All agency individuals are screened prior to authorizing access to agency information systems.
    2. All individuals are rescreened every **seven years**.
- **PS-4 Personnel Termination**

  Upon employee or contractor termination, the agency:
    a) Terminates information system access.
    b) Terminates/revokes any authenticators/credentials associated with the individual.
    c) Conducts exit interviews, as needed.
    d) Retrieves all security-related organizational information system-related property.

e) Retains access to organizational information and information assets formerly controlled by terminate personnel.
f) Notifies appropriate agency personnel upon termination of the employee.

- **PS-5 Personnel Transfer**
  1. Reassignment or transfer of agency employees is reviewed on a quarterly basis to include logical and physical access authorizations to information systems/facilities.
  2. Transfer or reassignment actions are initiated following the formal transfer actions.
  3. Access authorizations are modified as needed to correspond with any changes in employee operational needs due to reassignment or transfer.
  4. Designated agency personnel are notified of personnel transfer actions, as required.
- **PS-6 Access Agreements**
  1. Access agreements for agency information systems are maintained and reviewed at least **annually**.
  2. Individuals requiring access to organizational information and information systems are required to:
     a) Sign appropriate access agreements prior to being granted access
     b) Re-sign access agreements when access agreements have been updated or at least **annually**.
- **PS-7 Third-Party Personnel Security**
  1. Personnel security requirements including security roles and responsibilities for third-party providers are established and utilized for application to agency third party service providers.
  2. Third-party providers are required to comply with documented personnel security policies and procedures and security requirements established by the agency.
  3. Third-party providers are required to notify the agency of any of their personnel transfers or terminations who possess agency credentials or badges or who have information system privileges.
  4. Third party service provider compliance is required and monitored.
- **PS-8 Personnel Sanctions**
  1. The agency has implemented and adheres to a formal sanction process for personnel failing to comply with established information security policies and procedures.
  2. The sanctions process must be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance where applicable.

a) The sanctions process must also address the following:
    i. Informal corrective actions.
    ii. Formal disciplinary actions.
    iii. Severe disciplinary actions.
    iv. Removal of system access.
    v. Possible criminal and/or civil penalties
3. Designated agency personnel are notified when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

History

None

Evaluation

The Office of Information Technology (OIT), upon recommendation of the DHS Chief Information Security Officer (CISO), evaluates this policy annually by:

1. Comparing its content and intent to evolving regulatory compliance standards imposed upon the Agency, such as, IRS 1075, NIST 800-53, and CMS MARS-E.
2. Addressing any deficiencies or gaps discovered during periodic audits conducted by Georgia DOAA or other regulatory bodies, such as, IRS, CMS, SSA, FBI, etc.