	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1912 08/30/2019 08/30/2021

SUBJECT: DHS Information Security Policies

Security Awareness and Training

Policy

This policy establishes the Georgia Department of Human Services Enterprise Security Awareness and Training Policy, for managing risks from a lack of company security awareness, communication, and training through the establishment of an effective security awareness and education program. The security awareness and education program helps DHS document, communicate, and train the agency's employees on security best practices and concepts.

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

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 800-100 "Information Security Handbook: A Guide for Managers" March 2007
- United States Department of Commerce Technology Administration National Institute of Standards and Technology NIST Special Publication 800-12, An Introduction to Computer Security June 2017
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-16 "Information Security Training requirements: A Role- and Performance-Based Model" April 1998.
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-50 "Building an Information Technology Security Awareness and Training Program" September 2003.
- 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 has chosen to adopt the Security and Awareness principles established in NIST SP 800-16 "Information Technology Security Training Requirements: A Role- and Performance-Based Model." The following subsections outline the Security and Awareness standards that constitute DHS' policy. Each DHS Business System is then bound to this policy and must develop or adhere to a program plan which demonstrates compliance with the policy related to the standards documented.

- **AT-1 Security Awareness and Training Policy and Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing security awareness and training required by agency entities, and requirements for compliance.
    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 security awareness and training procedures shall be performed at least **annually**.
- **AT-2 Security Awareness**
    1. Basic security awareness training is provided to all information system users (including managers, senior executives, and contractors):
        A. As part of initial training for new user
        B. When required by information system changes
        C. At least **annually** thereafter
    2. The content of the basic information system security awareness training materials and security awareness techniques shall be determined based on specific requirements of the organization, federal regulations and the information systems to which personnel have authorized access.
        a) The content of DHS' security awareness program must include:
            i. A basic understanding of the need for information security.
            ii. User actions to maintain security.
            iii. User actions to respond to suspected security incidents.
            iv. Awareness of the need for operations security as it relates to the DHS' information security program.
    3. Security awareness training on recognizing and reporting potential indicators of insider threat is included and mandatory completion is required.

- **AT-3 Role-Based Security Training**
    1. Role-based security-related training is provided and is required as part of initial training for new users and is also when required by system changes.
    2. Role-base security training to personnel with assigned security roles and responsibilities is provided and required:
        a) Before authorizing access to the information system or performing assigned duties that require access to FTI
        b) When required by information system changes
        c) At least annually thereafter

        ** Personnel with security roles and responsibilities include, but are not limited to, the following positions: Information System Security Manager, Information System Security Officer, Security Specialist, Network Administrator, Systems Administrator, Database Administrator, Programmer/Systems Analyst, System Owner, Systems Designer/Systems Developer, helpdesk.
- **AT-4 Security Training Records:** All DHS Business Systems shall:
    1. Individual information system security training activities, including basic security awareness training and specific information asset security training, is documented and monitored.
    2. DHS employee security awareness and training records are retained for f**ive years.**

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.