	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1910 01/05/2022 01/05/2024

SUBJECT: DHS Information Security

Policies Planning Policy

POLICY

To establish and implement policies and procedures to ensure proper planning controls to the information system and information technology resources and any associated applications covered by federal, state and all other applicable rules and regulations, including the requirements establishing, documenting, reviewing, modifying and terminating individuals' right of access. Critical to achieving this objective is the implementation of controls that address each of the requirements stated in this policy.

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 800-100 "Information Security Handbook: A Guide for Managers" March 2007
- Federal Information Security Management Act of 2002 (FISMA)
- Georgia Technology Authority Enterprise Information Security Policy
- 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

Responsibilities

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

- **PL-1 Security Planning Policy and Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing authorized access and preventing unauthorized access to 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 planning procedures shall be performed at least **annually**.
- **PL-2 System Security Plan**
    1. The agency requires approved system security plans for all information systems.
        a) **FOR SYSTEMS WHICH PROCESS FTI DATA:** An approved Safeguard Security Report must be submitted to the IRS Office of Safeguards, and must be reviewed and updated (as necessary) at least **annually.**
        b) **FOR SYSTMES WHICH PROCESS SSA DATA:** An approved Security Design Plan must be submitted to the SSA, and must be reviewed and updated (as necessary) at least **annually.**
- **PL-4 Rules of Behavior**
    1. The agency has established, enforces, and makes readily available to individuals requiring access to the information system, rules of behavior which define, with regards to the information system:
        a) Their responsibilities
        b) Expected behavior
        c) Prohibited behavior
        d) Restrictions on social media/networking sites and posting agency information to public websites

****The IRS Office of Safeguards prohibits sharing FTI using any social media/networking sites.**

2. Prior to accessing being grated to the information system, all individuals must sign acknowledging that they have read the rules of behavior, which they shall abide by the rules therein.
3. 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**.
4. The Rules of Behavior are reviewed and updated (as necessary) at least **annually.**

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.