Office of Information Technology

1919 Personally Identifiable Information Processing and Transparency Policy

2025-10-20

Table of Contents

Policy . . . 2
Authority . . . 3
References . . . 4
Applicability . . . 5
Definitions . . . 6
Responsibilities . . . 7
- PT-1 Personally Identifiable Information Processing and Transparency Policy and Procedures . . . 7
- PT-2 Authority to Process Personally Identifiable Information . . . 7
- PT-3 Personally Identifiable Information Processing Purposes . . . 7
- PT-4 Consent . . . 8
- PT-5 Privacy Notice . . . 8
- PT-7 Specific Categories of Personally Identifiable Information . . . 9

History . . . 10
Evaluation . . . 11

	Department of Human Services **Online Directives Information System**	**Index:**	**POL1919**
		Revised:	**06/02/2025**
		Next Review:	**06/02/2027**

Subject: DHS Information Security Policies

Policy

This policy establishes the Personally Identifiable Information Processing and Transparency Policy, for managing risk associated with information assets, information leakage, and network vulnerabilities. The Personally Identifiable Information Processing and Transparency Policy and associated plans, augment DHS mission, by proactively identifying threats and vulnerabilities, which can result in consequences (impact).

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 – Administration of Children and Families (ACF), Office of Child Support Services (OCSS)
4. United States Department of Health & Human Services - Centers for Medicare & Medicaid Services (CMS)
5. Georgia Technology Authority
6. Social Security Administration
7. Federal Bureau Investigation (Criminal Justice Information 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 5, September 2020
- 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
- Social Security Administration (“SSA”) Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (“TSSR”)
- Criminal Justice Information Services Security Policy
- ACF/OCSS - Security Agreement

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 Personally Identifiable Information Processing and Transparency Policy and Procedures. The policy establishes a framework for the processing of Personally Identifiable information and ensures transparency in the management of risks associated with information assets, data breaches, and network vulnerabilities. The following subsections outline the Personally Identifiable Information Processing and Transparency 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 the standards documented.

PT-1 Personally Identifiable Information Processing and Transparency Policy and Procedures

a. Develop, document, and disseminate to **designated agency personnel**:

   A. All organizational level Personally Identifiable Information Processing and Transparency policy that:

      1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   B. Procedures to facilitate the implementation of the Personally Identifiable Information Processing and Transparency policy and the associated access controls;

b. Designate an **agency official** to manage the development, documentation, and dissemination of the Personally Identifiable Information Processing and Transparency policy and procedures; and

c. Review and update the current access control:

   A. Policy **every one (1) year (or if there is a significant change)**; and

   B. Procedures **every one (1) year (or if there is a significant change)**.

PT-2 Authority to Process Personally Identifiable Information

a. Determine and document the IRC § 6103 section that permits the receipt of personally identifiable information; and

b. Restrict the access of personally identifiable information to only that which is authorized

PT-3 Personally Identifiable Information Processing Purposes

a. Identify and document the organization-defined purpose(s) for processing Personally Identifiable Information (PII);

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the organization-defined processing of PII to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing PII and implement organization-defined mechanisms to ensure that any changes are made in accordance with organization-defined requirements.

PT-4 Consent

Implement organization-defined tools or mechanisms for individuals to consent to the processing of their Personally Identifiable Information (PII) prior to its collection that facilitate individuals' informed decision-making.

PT-4 (3) *Revocation:*

Implement organization-defined tools or mechanisms for individuals to revoke consent to the processing of their Personally Identifiable Information (PII).

PT-5 Privacy Notice

Provide notice to individuals about the processing of Personally Identifiable Information (PII) that:

a. Is available to individuals upon first interacting with an organization, and subsequently at organization-defined frequency;

b. Presents clear and easy to understand information about PII processing in plain language;

c. Identifies the authority that authorizes the processing of PII;

d. Identifies the purposes for which PII is to be processed; and

e. Includes any additional information the organization deems necessary to effect compliance with applicable laws, regulations, or policies.

PT-5 (1) *Just-In-Time Notice:*

Present notice of Personally Identifiable Information (PII) processing to individuals at a time and location where the individual provides PII or in conjunction with a data action, or at an organization-defined frequency.

PT-5 (2) *Privacy Act Statements:*

Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records or provide Privacy Act statements on separate forms that can be retained by individuals.

PT-7 Specific Categories of Personally Identifiable Information

Apply organization-defined processing conditions for specific categories of Personally Identifiable Information (PII).

History

Date	Change	User	Version

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.