Office of Information Technology

1921 Program Management Policy

2025-10-20

Table of Contents

	Department of Human Services **Online Directives Information System**	**Index:**	**POL1921**
		Revised:	**06/02/2025**
		Next Review:	**06/02/2027**

Subject: DHS Information Security Policies

Policy

The purpose of this policy is to provide oversight for organization-wide information security programs to help ensure the confidentiality, integrity, and availability of information processed, stored, and transmitted by DHS information systems. The Program Management family provides security controls at the organizational level rather than at the information system level.

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

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Responsibilities

a. DHS shall adopt the Program Management principles established in NIST SP 800-53 “Program Management,” Control Family guidelines, as the official policy for this domain. The following subsections outline the Program Management 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.

PM-1 Program Management Policy and Procedures

a. Develop and disseminate an organization-wide security program plan to **designated agency personnel**:
    1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities and compliance;
    3. Reflects the coordination among organizational entities responsible for information security; and
    4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, the state, and the Nation;
b. Protect the information security program plan from unauthorized disclosure and modification.
c. Review and update the current program management:
    A. Policy every **one (1) year (or if there is a significant change)**; and
    B. Procedures every **one (1) year, (or when there is a significant change)**.

PM-2 Information Security Program Leadership Role

Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

PM-3 Information Security and Privacy Resources

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;
b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and
c. Make available for expenditure, the planned information security and privacy resources.

PM-4 Plan of Action and Milestones Process

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:
    1. Are developed and maintained;
    2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
    3. Are reported in accordance with established reporting requirements.
b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-5 System Inventory

Develop and update continually an inventory of organizational systems.

PM-5 (1) *Inventory of Personally Identifiable Information:*

Establish, maintain, and update continually an inventory of all systems, applications, and projects that process personally identifiable information continuously or when there is a significant change to the systems, applications, and projects that process PII.

PM-6 Measures of Performance

Develop, monitor, and report on the results of information security and privacy measures of performance.

PM-7 Enterprise Architecture

Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

IRS.1:

Review and update the security enterprise architecture data based on the enterprise architecture timeframes.

PM-8 Critical Infrastructure Plan

Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

PM-9 Risk Management Strategy

a. Develops a comprehensive strategy to manage:
    1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
    2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
b. Implement the risk management strategy consistently across the organization; and
c. Review and update the risk management strategy at least every one (1) year or as required, to address organizational changes.

PM-10 Authorization Process

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;
b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
c. Integrate the authorization processes into an organization-wide risk management program.

PM-11 Mission and Business Process Definitions

a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
b. Determine information protection and Personally Identifiable Information (PII) processing needs arising from the defined mission and business processes; and
c. Review and revise the mission and business processes at least every three (3) years or when significant changes to mission and business occur.

PM-12 Insider Threat Program

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

PM-13 Security and Privacy Workforce

Establish a security and privacy workforce development and improvement program.

PM-14 Testing, Training and Monitoring

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

I. Are developed and maintained; and

II. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-15 Security and Privacy Groups and Associations

Establish and institutionalize contact with selected groups and associations within the security and privacy communities:

a. To facilitate ongoing security and privacy education and training for organizational personnel;

b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

c. To share current security and privacy information, including threats, vulnerabilities, and incidents.

PM-16 Threat Awareness Program

Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

PM-18 Privacy Program Plan

a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards;

b. Disseminate an organization-wide privacy program plan that provides an overview of the organization's privacy program; and

I. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;

II. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;

III. Includes the role of the senior official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;

IV. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;

V. Reflects coordination among organizational entities responsible for the different aspects of privacy; and

VI. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and

c. Review and update the policy and procedures at least every one (1) year or when there is a significant change.

PM-19 Privacy Program Leadership Role

Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

PM-20 Dissemination of Privacy Program Information

Maintain a resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior official for privacy;

b. Ensures that organizational privacy practices and reports are publicly available; and

c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

PM-20 (1) *Privacy Policies on Websites, Applications, and Digital Services:*

Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services that:

a. Are written in plain language and organized in a way that is easy to understand and navigate;

b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and

c. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

PM-21 Accounting of Disclosures

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

    1. Date, nature, and purpose of each disclosure; and

    2. Name and address, or other contact information of the individual or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five (5) years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

PM-22 Personally Identifiable Information Quality Management

Develop and document organization-wide policies and procedures for:

a. Reviewing for the accuracy, relevance, timeliness, and completeness of Personally Identifiable Information (PII) across the information life cycle;

b. Correcting or deleting inaccurate or outdated PII;

c. Disseminating notice of corrected or deleted PII to individuals or other appropriate entities; and

d. Appeals of adverse decisions on correction or deletion requests.

PM-25 Minimization of PII Used in Testing, Training, and Research

a. Develop, document, and implement policies and procedures that address the use of Personally Identifiable Information (PII) for internal testing, training, and research;

b. Limit or minimize the amount of PII used for internal testing, training, and research purposes;

c. Authorize the use of PII when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures at least every one (1) year.

PM-26 Complaint Management

Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:

a. Mechanisms that are easy to use and readily accessible by the public;

b. All information necessary for successfully filing complaints;

c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within thirty (30) working days from timestamp of submission, unless unusual or exceptional circumstances preclude completing action by that time;

d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within ten (10) working days from timestamp of submission; and

e. Response to complaints, concerns, or questions from individuals within thirty (30) working days from timestamp of submission, unless unusual or exceptional circumstances preclude completing action by that time.

PM-28 Risk Framing

a. Identify and document:

    1. Assumptions affecting risk assessments, risk responses, and risk monitoring;

2. Constraints affecting risk assessments, risk responses, and risk monitoring;
3. Constraints affecting risk assessments, risk responses, and risk monitoring; Priorities and trade-offs considered by the organization for managing risk; and
4. Constraints affecting risk assessments, risk responses, and risk monitoring; Organizational risk tolerance;

b. Distribute the results of risk framing activities to organization-defined personnel who have responsibilities for risk management; and

c. Review and update risk framing considerations at least every one (1) year or when a significant change occurs.

PM-29 Risk Management Program Leadership Roles

a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and

b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

PM-31 Continuous Monitoring Strategy

Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

a. Establishing organization-wide metrics to be monitored as defined by the organization;

b. Establishing organization-defined frequencies for monitoring and organization-defined frequencies for assessment of control effectiveness;

c. Ongoing monitoring of organizationally defined metrics in accordance with the continuous monitoring strategy;

d. Correlation and analysis of information generated by control assessments and monitoring;

e. Response actions to address results of the analysis of control assessment and monitoring information; and

f. Reporting the security and privacy status of organizational systems to organization-defined personnel or roles at least every thirty (30) days.

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.