	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1907 08/30/2019 08/30/2021

SUBJECT: DHS Information Security Policies

Media Protection Policy

POLICY

This policy establishes the Georgia Department of Human Services (DHS) Enterprise Media Protection Policy, for managing risks from media access, media storage, media transport, and media protection through the establishment of an effective Media Protection program. The Media Protection program helps DHS implement security best practices with regard to enterprise media usage, storage, and disposal.

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 800-60 “Guide for Mapping Types of Information and Information Systems to Security Categories” August 2008
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-111 “Guide to Storage Encryption Technologies for End User Devices” November 2007
- 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 National Institute for Standards and Technology (NIST) Special Publication 800-88 “Guidelines for Media Sanitization” Revision 1 December 2014
- 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, Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement, Version 1.0 August 2012

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

Media - Data storage material divided into three broad categories according to the recording method: (1) Magnetic, such as diskettes, disks, tapes, (2) Optical, such as microfiche, and (3) Magneto-Optical, such as CDs and DVDs

Sensitive Data – information that is protected against unwarranted disclosure, and requires specific safeguarding requirements. Sensitive data includes, but is not limited to, Federal Tax Information (FTI), Social Security Administration verified/provided information, Personally Identifiable Information (PII), Personal Health Information (PHI), etc.

Responsibilities
DHS shall adopt the Media Protection principles established in NIST SP 800-53 "Media Protection," Control Family guidelines, as the official policy for this domain. The following subsections outline the Media Protection 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 documented standards.

- **MP-1 Media Protection Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing media protection controls and preventing unauthorized access to IT resources, information systems, and media 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 media protection procedures shall be performed at least **annually**.
- **MP-2 Media Access**

  Access to sensitive data is restricted to authorized individuals.
- **MP-3 Media Marking**

  All removable information system media containing sensitive data is identified and labeled to indicate limits on distributions and handling parameters.
- **MP-4 Media Storage**
    1. DHS physically controls and securely stores digital (e.g., disks, magnetic tapes, external/removable hard drives, flash drives) and non-digital media (e.g., paper, microfilm), including media containing sensitive data, within secure areas using physical security controls and safeguards. Only agency approved/authorized media (both digital and non-digital) shall be authorized for use on the information system.
    2. DHS ensures the protection of information system media until the media is

destroyed or sanitized using contracted service provider approved equipment, techniques, and procedures.

a. The employment of cryptographic mechanisms shall be based upon maintaining the confidentiality and integrity of the information.
b. The strength of mechanisms shall be commensurate with the categorization and sensitivity of the information.
c. All digital storage (e.g., disks, magnetic tapes, external/removable hard drives, flash drives) shall employ a combination of encryption and password protection mechanisms. They shall encrypt data as soon as it is stored on the device with the full drive encryption feature.

- **MP-5 Media Transport**
    1. Digital (e.g., disks, magnetic tapes, external/removable hard drives, flash drives) and non-digital media (e.g., paper, microfilm) are protected and controlled during transport outside of controlled areas using service level agreements with contracted third party service providers, and by employing FIPS 1402- validated or compliant encryption technologies.
    2. Access of such media is restricted to authorized personnel, and accountability is maintained for information system media during transport outside of controlled areas by contracted third party service providers.
    3. All activities associated with the transport of information system media are documented— third party service providers are required to use transmittals or an equivalent tracking method to ensure sensitive data reach their intended destination.
- **MP-6 Media Sanitization**
    1. All media is sanitized, including media which contains sensitive data prior to releasing media to external agencies, disposal, and or re-use of media in accordance with the applicable regulatory guidance and policies.
    2. Sanitization mechanisms are employed with the strength and integrity commensurate with the security category or classification of the stored information.
    3. Contracted third party service providers are required to review, documents, and approves all media sanitation and disposal processes.

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.