	Department of Human Services Online Directives Information System	Index:	POL1909
		Effective:	09/20/2014
		Review:	11/02/2019

SUBJECT: DHS Information Security Policies

Physical and Environmental Protection Policy

POLICY

This policy establishes the Enterprise Physical and Environmental Protection Policy, for mitigating the risks from physical security and environmental threats through the establishment of an effective physical security and environmental controls program. The physical security and environmental controls program helps DHS protect its Information Technology Assets from Physical and Environmental threats.

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. Georgia Technology Authority
3. United States Internal Revenue Service
4. United States Department of Health & Human Services
5. 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, April 2013
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-73 “Interfaces for Personal Identity Verification” Revision 3 February 2010
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-76 “Biometric Data Specification of Personal Identity Verification” Revision 1 January 2007
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-78 “Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)” Revision 2 February 2010
- 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, Catalog of Minimum Acceptable Risk Controls 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 shall adopt the Physical and Environmental Protection principles established in NIST SP 800-53 "Physical and Environmental Protection," Control Family guidelines, as the official policy for this domain. The following subsections outline the incident 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 the standards documented.

- **PE-1 Physical and Environmental Protection Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing physical and environmental protection controls 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 physical and environmental protection procedures shall be performed **at least annually**.

- **PE-2 Physical Access Authorizations**
    1. A current list of personnel with authorized access to the facility or designated area within a facility where the information system resides must be kept.
        1. Those areas within the facility officially designated as publicly accessible are exempt from this requirement.
    2. Authorization credentials (e.g., badges, identification cards, and smart cards) must be issued.
        1. The level of access provided to each individual must not exceed the level of access required to complete the individual's job responsibilities.
            a) The level of access must be reviewed and approved.

2. Keys, badges, access cards, and combinations must be issued to only those personnel who require access.
3. Authorizations and requirements for access must be coordinated with facility and personnel security managers, as required or needed.

3. An approval process to 1) validate the appropriateness of physical access at these locations and 2) remove individuals from the facility access list when access is no longer required, is employed by agency in conjunction with third party service provider's implementation.
4. Physical access authorizations to the information system in addition to the physical access controls for the facility are utilized by agency third party service providers.
5. A periodic physical access review is conducted at least **annually.**

- **PE-3 Physical Access Control**
  1. All DHS Business Systems enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where information systems reside (excluding those areas within the facility officially designated as publicly accessible). This includes:
     a) Validation of individual access authorizations before granting access to the facility.
     b) Controlled entry to the facility containing the information asset using physical access devices and/or guards.
  2. Physical access audit logs for entry/exit points shall be maintained for auditing purposes.
  3. Visitors to DHS facilities shall be escorted at all times, and their activity shall be reviewed while on premises.
  4. Access to areas officially designated as publicly accessible are controlled in accordance with the agency's assessment of risk.
  5. Keys, combinations, and other physical access devices must be secured and inventoried annually.
     a) Coordination with facility management personnel must occur, where applicable.
  6. Combinations and keys must be changed on a routine basis.
     a) Combinations and keys must be changed immediately for reasons such as:
        i. Keys are lost.
        ii. Combinations are compromised.
        iii. Individuals are transferred, terminated, or no longer need access.
        iv. There is a theft or security violation in the area being protected.
     b) Coordination must occur with facility management personnel, as required.
  7. An inventory of physical access devices is performed on **annually**.

- **PE-4 Access Control for Transmission Medium**
    1. Physical access to information system distribution and transmission lines within organizational facilities is controlled.
    2. Protective measures to control physical access to information system distribution and transmission lines must include the following:
        a) Locked wiring closets.
        b) Disconnected or locked spare jacks.
        c) Protection of cabling by conduit or cable trays.
- **PE-5 Access Control for Output Devices**
    1. Physical access to information system output devices (e.g., monitors, printers, audio devices) must be controlled to prevent unauthorized individuals from obtaining the output.
        a) Methods to protect display devices include repositioning the monitor, and/or using a monitor filter.
- **PE-6 Monitoring Physical Access**
    1. Physical access to the information system must be monitored to detect and respond to physical security incidents.
        a) Coordination with facility management and personnel security management personnel must occur when responsibilities are in different organizations.
    2. Physical access logs are reviewed every **monthly.**
    3. The results of the reviews are disseminated to the agency's incident response team to address any issues found during the review.
    4. Physical intrusion alarms and surveillance equipment are monitored, and investigations performed if necessary for apparent security violations, suspicious physical access, etc.
- **PE-8 Visitor Control**
    1. Visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) must be maintained for a minimum of **5 years.**
    2. Visitor access records are reviewed at least **annually.**
- **PE-16 Delivery and Removal**
    1. Any and all types of information system components and packages that are delivered to or removed from the facility must be authorized, monitored, and controlled.
    2. Records of those items entering and exiting the facility must be maintained.
    3. Delivery areas must be restricted access areas and possibly isolated from the information system and media libraries in order to effectively enforce authorizations for entry and exit of information system components.

- **PE-17 Alternate Work Site**
    1. NIST based IT controls, such as the IRS Office of Safeguard requirements, Social Security Technical Security Requirements, Centers for Medicare and Medicaid Services requirements, etc., are employed at all at alternate work sites.
    2. A means for employees to communicate with information security personnel in case of security incidents or problems is available to all employees.
- **PE-18 Location of Information Asset Components**
  Information system components are positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

History

None