	Department of Human Services Online Directives Information System	Index: Effective: Review:	POL1915 09/20/2014 11/02/2019

SUBJECT: DHS Information Security Policies

System Maintenance Policy

POLICY

This policy establishes the Enterprise System Maintenance Policy, for managing risks from information asset maintenance and repairs through the establishment of an effective System Maintenance program. The system maintenance program helps DHS implement security best practices with regard to enterprise system maintenance and repairs.

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 800-63 “Electronic Authentication Guideline” December 2006
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Manager” October 2006
- Georgia Technology Authority Enterprise Information Security Policy
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication SP800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- Centers for Medicare & Medicaid Services’ Catalog of Minimum Acceptable Risk Controls for Exchanges
- United States Internal Revenue Service Publication 1075 “Tax Information Security Guidelines for Federal, State and Local Agencies

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

System maintenance - a catchall term used to describe various forms of computer or server maintenance required to keep a computer system running properly. It can describe network maintenance, which could mean that servers are being physically repaired, replaced, or moved. Network maintenance can also mean that the software for a server is being updated, changed, or repaired. This sort of maintenance is typically performed on a regular or semi-regular schedule, often during non-peak usage hours, and keeps servers running smoothly.

Responsibilities

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

- **MA-1 System Maintenance Policy and Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing system maintenance controls and preventing unauthorized access and maintenance on 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 system maintenance procedures shall be performed **at least annually**.
- **MA-2 Controlled Maintenance**
    1. Agency service providers schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with established organizational and applicable vendor requirements.
        a) The Maintenance Plan must address how the maintenance schedule is managed and the Point of Contact (POC) for scheduled maintenance.
    2. Agency services providers monitor and approve all on-site, remote, and alternate location maintenance activities.
    3. Removal of any information systems or system components must be approved by designated agency officials prior to off-site maintenance or repairs.

4. If off-site maintenance or repairs are required, all sensitive data, to include but not limited to, FTI and SSA data, and remaining data is sanitized from the component prior to removal from the data site.
5. Service providers are required to check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

- **MA-3 Maintenance Tools**
  All DHS service provider shall approve, control, and monitor the use of information asset maintenance tools.
- **MA-4 Non-Local Maintenance**
  All DHS service providers are required to:
  1. Explicitly authorize, monitor, and control non-local maintenance and diagnostic activities.
  2. Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information asset.
  3. Employ and require multi-factor identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions.
  4. Maintain records for non-local maintenance and diagnostic activities.
  5. Terminate all sessions and network connections when non-local maintenance is completed.
  6. Document policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.
- **MA-5 Maintenance Personnel**
  1. Established processed for maintenance personnel authorization are utilized and a current list of authorized maintenance organizations or personnel is maintained
     a) Agency service providers are required to ensure their member(s) are cleared prior to accessing the agency's information systems by following required policies and regulations.
  2. Service providers are required to ensure that personnel performing maintenance on the information asset must possess the required access authorizations.
     a) When maintenance personnel do not possess the required access authorizations, personnel with the required access authorizations and technical competence deemed necessary must be designated to supervise information system maintenance.
     b) Maintenance personnel who do not possess the required access authorizations must be escorted at all times while performing information system maintenance

3. Designated service provider personnel with required access authorizations and technical competence deemed necessary must supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
4. Ensure personnel does not remove property containing FTI or PHI unless it has been authorized.

- **MA-6 Timely Maintenance**
    1. Timely maintenance provisions (i.e., SLAs or equivalent language) must be included in all maintenance agreements for the information system.
        a) The timely maintenance provisions must cover maintenance support and/or spare or replacement parts for both routine maintenance and when there are failures, emergencies, or a need for unscheduled maintenance.
        b) The timely maintenance provisions must be expressed in terms of the timeframe from notification of the failure, emergency, or need for unscheduled maintenance.
        c) The provisions must address the timeframe for dispatching technicians.
        d) The maintenance agreements must define the security-critical information system components and/or key information technology components for which spare parts or replacement parts must be made available

DHS shall conduct system maintenance (Routine or Emergency) on all its Information Technology resources and environment. GTA and contracted Service Providers are responsible for performing DHS system maintenance as defined by Service Level Agreement (SLA) per the GETS service agreement.
All implementations, design, developments, repairs, updates or modifications of DHS information system components shall be reviewed and approved by the Chief Information Security Officer or the DHS Enterprise Architect.

History

None