	Department of Human Services Online Directives Information System	Index: Effective: Review:	POL1904 09/20/2014 11/02/2019

SUBJECT: DHS Information Security Policies

Contingency Planning Policy

POLICY

This policy establishes the Enterprise Contingency Planning Policy, for managing risks from information system disruptions, failures, and disasters through the establishment of an effective contingency planning program. The contingency planning program helps DHS implement security best practices with regards to enterprise business continuity and disaster recovery.

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
6. International Organization for Standardization

Reference

- 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
- Georgia Technology Authority Enterprise Information Security Policy
- 45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule: Contingency Plan 164.308(a)(7)(I)
- 45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule: Data Backup Plan 164.308(a)(7)(ii)(A)
- 45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule: Emergency Mode Operation Plan 164.308(a)(7)(ii)(C)
- 45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule: Contingency Operations 164.310(a)(2)(I)
- ISO 17799 Information Technology – Security Techniques Code of practice for information security management: 14.1.04 Business continuity planning framework
- ISO 27001 Information Technology – Security Techniques Information Systems Management Systems Requirements: A-14.1
- Centers for Medicare & Medicaid Services' Catalog of Minimum Acceptable Risk Controls for Exchanges
- 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

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

Recover Time Objectives (RTO) - the target time you set for the recovery of your IT and business activities after a disaster has struck.

Recover Point Objectives (RPO) - the maximum targeted period in which data might be lost from an IT service due to a major incident.

Responsibilities

DHS shall adopt the Contingency Planning principles established in NIST SP 800-34 "Contingency Planning Guide for Federal Information Systems," as the official policy for this domain. The following subsections outline the Contingency Planning 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.

- **CP-1 Contingency Planning Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing contingency planning procedures required for managing risks from disruptions 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 contingency planning procedures shall be performed at least **annually**.
- **CP-2 Contingency Plan**
    1. DHS has documented and executes an agency contingency plan for agency information systems that:
        a) Identifies essential missions and business functions and associated contingency requirements.
        b) Provides recovery objectives, restoration priorities, and metrics.
        c) Addresses contingency roles and responsibilities, to include contact information for individuals with assigned responsibilities;
            i. The plan shall include a detailed contact list. At a minimum, the contact list shall include primary (office) and secondary (home/personal) telephone numbers. The contact list shall also describe the contact escalation process. The contact list shall be reviewed annually as part of the CP review. The contact list shall also be updated out-of-cycle to address changes to CP personnel.

d) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.
e) Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented.
f) Is reviewed and approved by designated officials within the organization

2. Relevant system owners and key stakeholders are provided copies of the contingency plan.
3. Contingency planning activities with incident handling activities are coordinated amongst agency entities.
4. Review of the contingency plan for the information system is performed on an **annual** basis.
5. When necessary, the contingency plan is reviewed and updated to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
6. Contingency plan changes are communicated and distributed to relevant system owners and key stakeholders.
7. The contingency plan is protected from unauthorized disclosure and modification via implemented access controls.
8. Maintain all aspects of the CP to include:
   a) Updating the CP due to any changes to the system and the system environment that affect contingency and recovery operations. If changes have been made to the CP, they need to be communicated to all parties involved. Additionally, the updated CP shall be made available in hardcopy or softcopy, as applicable.
   b) Uploading the CP into the agency Information Security Repository. Subsequent updates to the plan will also be maintained and managed in the agency Information Security Repository

- **CP-3 Contingency Training**

DHS and their service providers train their personnel on their contingency roles and responsibilities with respect to the information system and provides refresher training:

1. Prior to assuming a contingency role or responsibility.
2. When required by information system changes.
3. **Annually** thereafter.

- **CP-4 Contingency Plan Testing and Exercises**

1. The agency maintains the effectiveness of the information system CP and readiness of the program office to execute the plan by:
   a) Developing a test plan and uploading it into the agency Information Security Repository;
   b) Performing annual testing using agency approved tests and exercises (checklist or table-top exercises);
   c) Testing the CP for all new systems prior to production deployment;

d) Documenting in the agency Information Security Repository and reviewing CP test results; and
e) Documenting in the agency Information Security Repository and implementing corrective actions.
    i. Significant deficiencies shall be remediated prior to production deployment.
    ii. Corrective actions shall be documented using the Plan of Action and Milestones (POA&M) in the agency Information Security Repository.

2. Senior management, management, and key stakeholders review the contingency plan test/exercise results in order to initiate corrective actions, if needed.

- **CP-6 Alternate Storage Site**
    1. The agency utilizes an alternate storage site, which includes necessary agreements to permit the storage and recovery of information system backup information.
    2. The alternate storage sites provides information security safeguards which meet the minimum protection standards and the disclosure provisions of IRC 6103.
    3. The alternate site for storage and recovery of the information system's backup information is established with the following requirements, but are not limited to:
        a) Service and Support Agreements shall be in place with the alternate storage site and uploaded into the agency Information Security Repository.
            i. The agreements shall detail service levels to be provided.
            ii. The agreements shall include confidentiality requirements per federal guidelines.
        b) The CP for the information system shall include the following:
            i. Alternate storage site location: street address, city/town, state, zip code, and site contact information.
            ii. Terms of use for the alternate storage site.
            iii. Hazards or risks associated with the alternate storage site and mitigations to address them.
            iv. Mitigation actions to address potential problems associated with physically accessing the alternate storage site.
        c) A log of all information system backup data stored at, or retrieved from, the alternate storage facility shall be maintained
- **CP-7 Alternate Processing Site**
    1. An alternate processing site is utilized by the state, which includes necessary agreements to permit the transfer and resumption of information system operations for essential missions and business functions within defined **recovery time objectives** (RTO) **and recovery point objectives** (RPO) when the primary processing capabilities are unavailable.
    2. All equipment and supplies at the alternate processing site are required to ensure that the resumption of operations is available at the alternate site, and that contracts are in place

to support delivery to the site in time to support the organization-defined time period for resumption.

- **CP-8 Telecommunications Services**
  DHS utilizes alternate telecommunications services, which include the necessary agreements to permit the resumption of information system operations for essential missions and business functions within **defined recovery time and recovery points** when the primary telecommunications capabilities are unavailable.
- **CP-9 Information System Backup**
  1. Backup data residing on information systems including, but not limited to, the following:
     a) Backups of user-level information contained in the information system shall be conducted at least weekly.
     b) Backups of system-level information contained in the information system shall be conducted at least weekly. System-level information includes, for example, system state information, operating system and application software, and licenses.
     c) Backups of information system documentation including security-related documentation shall be conducted at least weekly.
     d) The frequency of information system backups shall be consistent with the information systems' RTOs and RPOs.
     e) The confidentiality and integrity of the system backup information shall be protected at the storage location.
        i. Sensitive information such as the information system's assessment of risk and similar information content shall determine the use of encryption or other measures for protecting backup information.
     f) Information systems that include backups of sensitive personally identifiable information (SPII) shall use an encryption module that is certified to meet Federal Information Processing Standards (FIPS) 140-2.
     g) Procedures for backing up and restoring the information system shall be documented and included in, or as attachments to, the information system CP.
     h) Backup and restoration procedures shall address the following:
        i. A routine schedule shall be established for backing up user-level and system-level information.
        ii. All backup media shall include markings that address the contents of the media; date created, and sequence number, if multiple media were used. Refer to the DHS Information Security – Media Protection Procedures document for requirements on media protection.
        iii. The priorities and sequencing of restoration shall be established.
  2. The confidentiality and integrity of backup information is implemented and maintained at the storage location pursuant to IRC 6103 requirements.

- **CP-10 Information System Recovery and Reconstitution**
  DHS recovers and reconstitutes information systems to a known state after a disruption, compromise, or failure.

History
None