2016

Department of Social Services

INFORMATION SECURITY POLICY:
CONTINGENCY PLANNING

Contents

1. INTRODUCTION

1.1 Document Versioning Control

The history of revisions, modifications, and changes to this document should be documented and reflected in this section.

Last Reviewed:	**Effective Date: 8/22/2016**
Reviewed By: DSS CISO	**Next Review: 08/21/2017**
Date Approved: 8/22/2016	**Authority: DSS CISO**
Approved By: DSS CIO	**Policy Owner:**
Supersedes:	**Policy Number:**

Version	Sections Revised	Description of Revisions	Changed By	Date
1.0	All	Initial Document Creation	Clifford Callender	4/01/16
2.0	All	Revised Document Based on Initial Review Comments from DSS	Clifford Callender	7/14/16
3.0	All	Final Document Based on Final Review Comments from DSS	Clifford Callender	8/19/16

1.2 Purpose

The Contingency Planning (CP) family provides controls to guide the agency's information security contingency planning program. This policy establishes the requirements that manage the risks derived from information asset disruptions, failures, and disasters through the establishment of business continuity and disaster recovery controls. This policy, in conjunction with the other information security policies, will be used to construct, implement, and support the information security program across the Department of Social Services (DSS). Section 2 of the Master Governance Policy further defines the purpose of the DSS information security and privacy policies.

1.3 Scope

All DSS employees, contractors, and business partners are responsible for understanding and complying with this policy. This policy applies to all current and future systems and processes handling DSS data. Section 3 of the Master Governance Policy further defines the scope of this policy.

1.4 Roles and Responsibilities

The following roles are responsible for implementing, distributing, enforcing, maintaining, or otherwise supporting this policy:

- D.1, The Committee Chair DSS Commissioner
- D.2, The Agency Risk Management Steering Committee
- D.3, The DSS Chief Information Officer (CIO)
- D.4, The Committee Chair Information Technology Services (ITS) CIO
- D.5, D.8 The Chief Information Security Officer (CISO)
- D.6, The Committee Co-Chair DSS Deputy Commissioner
- D.7, Committee Chair Information Technology Services (ITS) Chief Information Officer (CIO)
- D.9, The Business Owners and Information Technology (IT) Custodians
- D.10, The System Managers/Application Administrators/Technical Administrators and Managers
- D.11, Agency Security Review Committee
- D.12, All Tactical, Technical, and Operational Level Individuals

While these roles are an integral part of this policy, it is the responsibility of all DSS personnel to promote a strong security posture. For more information regarding the responsibilities, owners, and structure of these roles, please see Section 4 of the Master Governance Policy.

1.4.1. Management Commitment

DSS management is committed to promoting security within the organization through clear direction, demonstrated commitment, explicit assignment, promotion of a strong security culture and awareness, and acknowledgment of information security responsibilities. Section 4.1 of the Master Governance Policy provides more details on the management commitment statement for the DSS information security and privacy policies.

1.4.2. Coordination among Organizational Entities

The following organizational entities have a role in the implementation, distribution, enforcement, maintenance, or support of this policy.

- N.1, Office of Organizational and Skill Development (OSD)
- N.3, Legal Counsel
- N.4, Users
- N.5, DSS Operations
- N.6, DSS Information Technology Services (ITS) Operations
- N.7, DAS-BEST
- N.9, Legal
- N.13, Privacy Officer
- N.17, Contracts
- N.21, DSS Microsystems

While these listed organizational entities are an integral component of this policy, it is the responsibility of the organizations within DSS to support a strong security posture. Section 4.2 of the Master Governance Policy defines the coordination among organizational entities for this policy.

1.5 Compliance

Violations of this policy may lead to revocation of system privileges and/or disciplinary action up to and including termination. Section 6 of the Master Governance Policy further defines the compliance requirements of this policy.

1.6 References

The sections below list the internal and external artifacts that are referenced by this policy.

1.6.1. External

This policy references the following external laws, regulations, and industry standards:

- Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E v. 2.0) – System Security Plan (SSP)
- Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules
- Internal Revenue Service (IRS) Publication 1075 (IRS 1075) (October 2014) – Safeguard Security Report (SSR)
- The United States Social Security Administration (SSA) Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information (SSA EIE) – Security Design Plan (SDP)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4

1.6.2. Internal

This policy references the following internal policies, procedures, standards, guidelines and methodologies:

- DSS CP Procedure(s)
- DSS Governance Policy
- Legacy: IT Contingency and Disaster Recovery Planning Standard Operating Procedure
- Legacy: DSS Risk Management Framework Security Planning Approval Process
- Legacy: DSS Information Security Processes, Policies, and Procedures Guide
- Legacy: DSS IT Contingency and Disaster Recovery Planning Guide

1.7 Maintenance

This policy and its supporting procedures, standards, and guidelines, will be reviewed annually and updated as needed. A record of the updates can be found in Section 1.1, Document Versioning Control of this policy. Section 8 of the Master Governance Policy further defines the maintenance requirements of this policy.

2. INFORMATION SECURITY POLICY

2.1 Contingency Planning

DSS has chosen to adopt the moderate-impact baseline controls established in the NIST SP 800-53 Rev.4 Contingency Planning (CP) control family as the framework for this policy. The following subsections outline the Contingency Planning control requirements that constitute the DSS CP policy.

Policy	[CP-1] Contingency Planning Policy and Procedures
	• [CP-1] DSS shall develop, document, and disseminate to applicable personnel:
	  o A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
	  o Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
	• [CP-1] DSS shall review and update the current:
	  o Contingency planning policy within every three hundred sixty-five (365) days;
	  o Contingency planning procedures within every three hundred sixty-five (365) days.
	• [IRS 1075 – §9.3.6]: DSS shall develop applicable contingencies to make Federal Tax Information (FTI) available to carry out its mission.
	• [HIPAA – §164.308(a)(7)(i)]: DSS shall establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information.
	• Legacy: Contingency Planning baselines will be continuously reviewed and evaluated. Baselines will be updated as required to ensure that IRS, HIPAA and SSA compliant control capabilities will be maintained. Supporting methodologies and procedures will provide specific guidelines and instructions to ensure the effective implementation of required security controls and control enhancements in the NIST SP 800-53 Contingency Planning control family. Methodologies and procedures in support of required NIST 800-53 Contingency Planning control element definitions will be developed, documented, approved and disseminated in accordance with the DSS Risk Management Framework Security Planning Approval Process for all information systems storing, accessing, processing or transmitting State of Connecticut or Federal Government data. Roles, responsibilities and coordination among DSS entities will be established in accordance with approved definitions documented within the DSS Risk Management Framework Security Planning Approval process. Methodologies and procedures will include specific references and mappings to required NIST 800-53 control elements required to meet

	regulatory compliance. [CP-2, CP-2(1), CP-(3), CP-(8)] Contingency Plan • [CP-2]: DSS shall develop a contingency plan for information systems in accordance with NIST SP 800-34 that: o Identifies essential organizational missions and business functions and associated contingency requirements; o Provides recovery objectives, restoration priorities, and metrics; o Addresses contingency roles, responsibilities, assigned individuals with contact information; o Addresses maintaining essential organizational missions and business functions despite an information system disruption, compromise, or failure; o Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; o Is reviewed and approved by designated DSS officials. • [CP-2]: DSS shall distribute copies of the contingency plan to the Information System Security Officer, Business Owners, Contingency Plan Coordinator, CMS, IRS, SSA, and other stakeholders identified within the contingency plan. • [CP-2]: DSS shall coordinate contingency planning activities with incident handling activities. • [CP-2]: DSS shall review the contingency plan for the information system within every three hundred sixty-five (365) days. • [CP-2]: DSS shall update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. • [CP-2]: DSS shall communicate contingency plan changes to contingency personnel and organizational elements identified above. • [CP-2]: DSS shall protect the contingency plan from unauthorized disclosure and modification. • [MARS-E – §CP-2]: DSS shall define a list of contingency personnel (identified by name and/or by role) and organizational elements for distribution and receipt of the contingency plan and contingency plan changes. The contingency list shall include designated CMS personnel. • [HIPAA – §164.308(a)(7)(ii)(B)]: DSS shall establish (and implement as needed) procedures to restore loss of data. • [HIPAA – §164.308(a)(7)(ii)(C)]: DSS shall establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

	• [HIPAA – §164.308(a)(7)(ii)(E)]: DSS shall assess the relative criticality of specific applications and data in support of other contingency plan components. • [SSA EIE – §4.0]: In accordance with NIST SP 800-34, DSS shall document an approved contingency plan that includes a disaster recovery plan that addresses both natural disaster and cyber-attack situations. • [SSA EIE – §4.0]: The DSS contingency plan shall include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that address the security of SSA-provided information if a disaster occurs. • [CP-2(1)]: DSS shall coordinate contingency plan development with organizational elements responsible for related plans. • [MARS-E – §CP-2(2)]: DSS shall conduct capacity planning to provide the required capacity for information processing, telecommunications, and environmental support during contingency operations. • [CP-2(3)]: DSS shall plan for the resumption of essential missions and business functions within the Maximum Tolerable Downtime (MTD), determined by the business owner, for the business functions. • [CP-2(8)]: DSS shall identify critical information system assets supporting essential missions and business functions. • Legacy: The Deputy Commissioner-DSS Programs will assign appropriate personnel to complete the Business Impact Analysis step, Section 3, of the DSS IT Contingency and Disaster Recovery Planning Standard Operating Procedure for all applications and systems utilizing HIPAA, FTI, IRS and HHS data. The Manager of ITS Operations will address Section 4.0, Anticipation of potential contingencies or disasters, to identify significant threats and develop scenarios to defend DSS applications, systems, hardware and software. In this process the manager of ITS Operations will reach out to DAS/BEST, DRS and all relevant federal agencies to determine their needs and receive their input. Based on his findings, the Manager of ITS Operations will develop strategies based on Section 6.0 Selection of contingency planning strategies. [CP-3] Contingency Training • [CP-3]: DSS shall provide contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities: o Prior to assuming a contingency role or responsibility; o When required by information system changes; o And every six (6) months thereafter. [CP-4, CP-4(1)] Contingency Plan Testing • [CP-4]: DSS shall test the contingency plan for the information system within every six (6) months using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan.

	• [CP-4]: DSS shall review the contingency plan test results. • [CP-4]: DSS shall initiate corrective actions, if needed. • [MARS-E – §CP-4]: DSS shall produce an after-action report to improve existing processes, procedures, and policies. • [HIPAA – §164.308(a)(7)(ii)(D)]: DSS shall implement procedures for periodic testing and revision of contingency plans. • [CP-4(1)]: DSS shall coordinate contingency plan testing and/or exercises with organizational elements responsible for related plans. • Legacy: The Manager of ITS Operations will utilize Section 7.0 of the DSS IT Contingency and Disaster Recovery Planning Guide to test all plans annually and advise the Deputy Commissioner-DSS Programs of any changes to the plans based on test results. All state and federal agencies providing data or services to DSS will be polled to ensure that DSS plans are coordinated with existing or updated plans. The Deputy Commissioner DSS-Programs shall maintain the latest contingency plans for use when needed. [CP-6, CP-6(1), CP-6(3)] Alternate Storage Site • [CP-6]: DSS shall establish an alternate storage site and the required agreements to permit the storage and retrieval of information system backup information. • [CP-6]: DSS shall require that the alternate storage site provide information security safeguards equivalent to that of the primary site. • [IRS 1075 – §9.3.6.5]: DSS shall require that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of Internal Revenue Code (IRC) 6103. • [CP-6(1)]: DSS shall identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats. • [CP-6(3)]: DSS shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. • Legacy: As a function of completing Section 4.0 tasks, the Manager of ITS Operations will develop contingent alternate storage sites for all applications and systems which require them. Such sites will be located in areas outside the hazard area of the DSS facilities. Such sites must be accessible to required DSS staff in the event of a disaster. [CP-7, CP-7(1), CP-7(2), CP-7(3)] Alternate Processing Site • [CP-7]: DSS shall establish an alternate processing site, including required agreements to permit the transfer and resumption of information system operations, for essential missions/business functions in accordance with the agency's contingency plan when the primary processing capabilities are unavailable. • [CP-7]: DSS shall require that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site to permit resumption of

	essential missions and business functions within a resumption time period consistent with the recovery time objectives defined by the business owner in the contingency plan. • [CP-7]: DSS shall require that the alternate processing site provides information security safeguards equivalent to those of the primary site. • [IRS 1075 – §9.3.6.6]: DSS shall require that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103. • [HIPAA – §164.310(a)(2)(i)]: DSS shall establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. • [CP-7(1)]: DSS shall identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats. • [CP-7(2)]: DSS shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. • [CP-7(3)]: DSS shall develop alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). • Legacy: As a function of completing Section 4.0 tasks, the Manager of ITS Operations will develop contingent alternate processing sites for all applications and systems which require them. Such sites will be located in areas outside the hazard area of the DSS facilities. Such sites must be accessible to required DSS staff in the event of a disaster. If the processing site is co-located or located in commercial space, DSS must have alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements and that security measures are equivalent to DSS' primary site. [CP-8, CP-8(1), CP-8(2)] Telecommunications Services • [CP-8]: DSS shall establish alternate telecommunications services including the required agreements to permit the resumption of information system operations for essential organizational missions and business functions within an organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. • [MARS-E – §CP-8]: DSS shall require that alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business function Maximum Tolerable Downtimes (MTD). • [MARS-E – §CP-8]: DSS shall define a resumption time period consistent with the RTOs and business impact analysis. The time period shall be approved and accepted by the business owner. • [CP-8(1)]: DSS shall develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in

	accordance with organizational availability requirements (including recovery time objectives). • [CP-8(1)]: DSS shall request telecommunications service priority for telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. • [CP-8(2)]: DSS shall obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services. [CP-9, CP-9(1)] Information System Backup • [CP-9]: DSS shall conduct backups of user-level information, system-level information, and security-related documentation contained in the information system in accordance with the organization-defined frequency consistent with recovery time and recovery point objectives in the contingency plan. • [CP-9]: DSS shall conduct backups of system-level information contained in the information system in accordance with the organization-defined frequency consistent with recovery time and recovery point objectives in the contingency plan. • [CP-9]: DSS shall conduct backups of information system documentation including security-related documentation, others forms of data, and paper records within the frequency defined in the applicable SSP, consistent with recovery time and recovery point objectives in the contingency plan. • [IRS 1075 – §9.3.6.7]: DSS shall protect the confidentiality, integrity, and availability of backup information at storage locations pursuant to IRC 6103 requirements. • [MARS-E – §CP-9]: DSS shall perform full backups weekly to separate physical media and incremental or differential backups daily to separate physical media. Backups shall include user-level and system-level information (including system state information). Three (3) generations of backups or more (full as well as the related incremental or differential backups) shall be stored off site. Off-site and on-site backups shall be logged with name, date, time and action. • [MARS-E – §CP-9]: DSS shall require that a current, retrievable, copy of Personally Identifiable Information (PII) be available before movement of servers. • [MARS-E – §CP-9]: DSS shall determine what elements of the cloud environment require the information system backup controls listed above. • [MARS-E – §CP-9]: DSS shall determine how information system backup controls will be verified in cloud environments and the appropriate periodicity of the check. • [HIPAA – §164.308(a)(7)(ii)(A)]: DSS shall establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. • [CP-9(1)]: DSS shall test backup information following the backup to verify

	media reliability and information integrity. • [MARS-E – §CP-9(1)]: DSS shall test backup information at least annually. • [IRS 1075 – §4.4]: Handling FTI shall be such that the documents do not become misplaced or available to unauthorized personnel. When FTI is transported from one location to another, care shall be taken to provide appropriate safeguards. When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it shall be kept with that individual and protected from unauthorized disclosures. • [IRS 1075 – §4.4]: Paper and electronic FTI transported through the mail or courier/messenger service shall be documented on a transmittal form and monitored so that each shipment is properly and timely received and acknowledged. It shall also be double-sealed with the inner envelope marked "confidential" with some indication that only the designated official or delegate is authorized to open it. • [IRS 1075 – §4.4]: Shipments of paper FTI and electronic FTI (including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes, and microfilm) shall be documented on a transmittal form and monitored so that each shipment is properly and timely received and acknowledged. FTI transported through the mail or courier/messenger service shall be double-sealed, with the inner envelope or box marked "confidential" with some indication that only the designated official or delegate is authorized to open it. [CP-10, CP-10(2)] Information System Recovery and Reconstitution • [CP-10]: DSS shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner. • [MARS-E – §CP-10]: Secure information system recovery and reconstitution shall include, but shall not be limited to: o Reset system parameters (either default or organization-established); o Reinstall patches; o Reestablish configuration settings; o Reinstall application and system software; o Fully test the system. • [CP-10(2)]: DSS shall implement transaction recovery for systems that are transaction-based. • Legacy: The DSS Manager of ITS will develop procedures to ensure that: o All DSS information systems that are transaction-based implement transaction recovery; o There are compensating security controls for any circumstances that can inhibit recovery and reconstitution to a known state.