# Table of Contents

I. DOCUMENT REVISION CONTROL – ANNUAL REVIEW ................................................... 1

II. RECORD OF CHANGES ............................................................................................... 2

III. DOCUMENT PURPOSE, SCOPE, SITUATIONS AND CONSIDERATIONS ............... 3
   A. PURPOSE .................................................................................................................... 3
   B. DOCUMENT SCOPE .................................................................................................. 3
   C. AUTHORITY ................................................................................................................ 4
   D. SITUATION .................................................................................................................. 4
   E. PLANNING CONSIDERATIONS ................................................................................. 5
   F. OBJECTIVES ............................................................................................................. 5
   G. SECURITY AND PRIVACY STATEMENT .................................................................... 6

IV. CONCEPT OF OPERATIONS ..................................................................................... 7
   A. PHASE I: READINESS AND PREPAREDNESS (PRE-ACTIVATION) ............................... 7
      Organization Readiness and Preparedness .................................................................. 7
      Staff Readiness and Preparedness .............................................................................. 7
      Agency Day to Day Preparations .............................................................................. 8
      Agency Functions, Service and Process Continuity Priorities ................................... 8
   B. PHASE II: ACTIVATION ......................................................................................... 10
      DSS Incident Command Team (ICT) ......................................................................... 10
      ICT Roles and Responsibilities .............................................................................. 11
      Field Operations ....................................................................................................... 16
      Decision Process Matrix ......................................................................................... 16
      Alert and Notification Procedures ....................................................................... 17
      Communications ...................................................................................................... 18
      Emergency Command Center (ECC) ....................................................................... 22
      Relocation Operations ............................................................................................. 22
      Field Operations Relocation .................................................................................... 23
   C. PHASE III: CONTINUITY OPERATIONS ................................................................ 25
   D. PHASE IV: RECONSTITUTION OPERATIONS ....................................................... 26

V. IDENTIFICATION OF ESSENTIAL FUNCTIONS ....................................................... 26

VI. IDENTIFICATION OF CONTINUITY PERSONNEL .................................................. 27

VII. TEST, TRAINING, AND EXERCISES PROGRAM .................................................... 27

ANNEX A: INFORMATION TECHNOLOGY SERVICES (ITS) ............................................ 28
   A.1 Business Continuity / Disaster Recovery Plan Development .................................... 28
   A.2 Team Call List ........................................................................................................ 28
   A.3 Business Continuity Objectives ............................................................................. 28
   A.4 ITS Disaster Assumptions ..................................................................................... 28
   A.5 Data Considerations – Disclosure of Information to Federal, State or Local Agencies (DATA) ......................................................... 28
   A.6 Business Continuity / Disaster Recovery Scenario Narratives ................................ 28
   A.7 Roles and Responsibilities ..................................................................................... 28
   A.8 Processes ............................................................................................................... 30
   A.9 Dependencies ....................................................................................................... 30
   A.10 Servers Managed by DAS – BEST for DSS ......................................................... 30
   A.11 Servers Managed by DSS .................................................................................... 30
A.12 Telephony Servers Managed by DSS
A.13 Non-Critical Telephony Servers for post recovery (i.e. systems that will be restored when time permits)
A.14 Switch Information
A.15 Data maintained outside of DSS resources
A.16 Access Health CT
A.17 Servers Backup Information

GLOSSARY
REFERENCES
I. DOCUMENT REVISION CONTROL – ANNUAL REVIEW

Annually, the Department of Social Services (DSS) will review this Business Continuity/Disaster Recovery Plan and make any required updates or changes.

Date of Original Business Continuity/Disaster Recovery Plan Acceptance: 31 March 2018

Annual Maintenance Recertification

<table>
<thead>
<tr>
<th>Year</th>
<th>Date of Recertification</th>
<th>Certified By</th>
<th>Title</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>04/10/2019</td>
<td>CISO</td>
<td>DSS CISO</td>
<td>Signed</td>
</tr>
</tbody>
</table>
## II. RECORD OF CHANGES

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Section</th>
<th>Date of Change</th>
<th>Change POC</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>All</td>
<td>3/31/2018</td>
<td></td>
<td>Initial document development</td>
</tr>
</tbody>
</table>
III. DOCUMENT PURPOSE, SCOPE, SITUATIONS AND CONSIDERATIONS

A. Purpose

The purpose of this document is to provide direction to the Connecticut Department of Social Services (DSS) in responding to a contingency event at the Department of Social Services Central Office at 55 Farmington Ave, Hartford, CT, one of the regional service centers located throughout Connecticut or the state data centers in CT or MA. It will assist in ensuring critical business functions are continued without an unacceptable delay or disruption. While the severity and consequences of an emergency cannot be predicted, effective contingency planning can minimize the impact on the DSS missions, personnel, and facilities.

The current changing threat environment and recent emergencies, including acts of nature, accidents, technological emergencies, and terrorist attack-related incidents, have increased the need for viable continuity capabilities and plans that enable organizations to continue their essential functions in an all-hazards environment and across a spectrum of emergencies. Today’s threats have emphasized the importance of programs that ensure continuity throughout all levels of governments.

This document is important because the impact of DSS’ mission goes well beyond the walls of its facilities. The DSS mission is to provide a wide array of health and human services to approximately 1 million Connecticut residents of all ages. In order to provide these services, DSS uses a variety of data elements that includes but is not limited to personally identifiable information (PII), protected health information (PHI), and other sensitive data elements. Many citizens of Connecticut rely on the services provided by DSS to assist in meeting their basic human needs. It is therefore vitally important for the information contained herein to be documented and regularly updated.

B. Document Scope

This document is developed to be the DSS Business Continuity/Disaster Recovery Plan for the DSS location at 55 Farmington Ave, Hartford, CT and DSS field offices unless otherwise stated. Certain DSS functions may involve additional state organizations. One example is the DSS reliance on the state data centers. Those circumstances will be identified where applicable.

This scope of this document does not include providing business continuity strategies for financial controls. Rather, it is intended to address the confidentiality, integrity and availability of the systems and data that are under DSS responsibility.

Additionally, this document does not supersede other DSS Continuity or Contingency Plans developed by divisions for specific purposes, such as the Pandemic Continuity of Operations...
Plan. Rather it is intended to augment those plans by aligning functions, processes and responsibilities as much as possible.

C. Authority

As specified in the State of Connecticut State Response Framework Version 4.1 September 2014; Title 28, Chapter 517 of the Connecticut General Statutes is the major source of authority for the State of Connecticut and its political subdivisions to prepare for and respond to natural disasters and other emergencies. This document does not supersede any of the requirements set forth in the State of Connecticut State Response Framework, but rather enhances the guidance for the Department of Social Services.

This plan was developed to align with the procedures and priorities established in the Department of Social Services Influenza Pandemic Continuity of Operations Plan. Though the plan specifies Influenza Pandemic in its title, it is a comprehensive plan that best documents DSS processes and service restoration priorities across the entire Agency. Additionally, the plan has been updated and tested for nearly a decade.

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, PL 100-707, signed into law November 23, 1988, which amended the Disaster Relief Act of 1974, PL 93-288, (the Stafford Act) is the federal legislation that creates a national program for disaster preparedness, response, recovery, and mitigation. Connecticut’s emergency management program, developed under the authority of Title 28, complies with the federal program established by the Stafford Act.

To that end, by continuing the performance of essential functions through a catastrophic emergency and ensure that essential services are provided to the Nation’s citizens. A comprehensive and integrated continuity capability will enable a more rapid and effective response to, and recovery from, an emergency.

D. Situation

Continuity planning should be based on the assumption that under most circumstances organizations will not receive warning of an impending emergency. Many natural, man-made and technological emergencies should be considered while developing an organizations’ continuity plan. Examples of natural emergencies include: Hurricanes, Blizzards/Winter Storms, Tornadoes, Floods, Fires, Earthquakes or widespread health-related concerns. Examples of man-made hazards include (but are not limited to) terrorism, widespread power failure or hazards associated with nuclear power plants in and around Connecticut. Lastly, Cyber threats such as a major Distributed Denial of Service (DDoS) attack, widespread malware proliferation or other unforeseen activity may severe impacts that share the disruptive capabilities of natural or man-
made emergencies. It is also possible that combinations of these hazards may exist as well in certain circumstances.

E. Planning Considerations

This Business Continuity / Disaster Recovery Plan has been developed to coincide with the priorities of the Department of Social Services recognizing that disasters can take any number of different paths. This plan addresses the Agency’s priority functions and services to the residents of the State of Connecticut. **In the event of a disaster or incident, the Department of Social Services will focus its resources and efforts on the continued provisions of cash, food, medical and crisis intervention services for new and existing clients and take appropriate steps towards the protection of the health and safety of its staff in the workplace.**

This Continuity Plan is based on the following considerations:

- The main scenarios to be considered as part of this plan are:
  - A disaster / incident at the main DSS physical facility (i.e. 55 Farmington Ave., Hartford) which renders this facility inaccessible or uninhabitable
  - A disaster / incident at a DSS field site which renders a facility or facilities inaccessible or uninhabitable
  - A loss of IT support and computer services due to a disaster / incident at the state data facility in CT or MA which disrupts data services to DSS facilities

- Emergency planning is based on pre-incident identification of at-risk processes and systems and the determination of resource shortfalls and contingencies. The *Influenza Pandemic Continuity of Operations Plan* provides a comprehensive list of at-risk processes and systems across the DSS enterprise and should be considered as the comprehensive source document for DSS processes.

- A disaster or emergency can occur with little or no warning, and can escalate to exceed the response capability of any single local authority or responding organization.

- The purpose of State government and its respective agencies and subdivisions during incidents and emergency situations is to assist local jurisdictions in providing for residents and visitors based on the following priorities: life safety, incident stabilization, and property conservation—in that order.

F. Objectives

The continuity planning objectives for non-federal agencies are identified in CGC 1, Continuity Guidance for Non-Federal Governments (States, Territories, Tribal, and Local Government Jurisdictions), dated July 2013.¹

- The DSS continuity objectives are listed below:
1) Reducing the loss of life and minimizing property damage and loss.
2) Ensuring that the organization can perform its essential functions under all conditions.
3) Reducing or mitigating disruptions to operations.
4) Protecting personnel, facilities, equipment, records, and other assets critical to the performance of essential functions in the event of a disruption.
5) Executing a successful order of succession with accompanying authorities in the event a disruption renders that organization’s leadership unable, unavailable, or incapable of assuming and performing their authorities and responsibilities of office.
6) Ensuring there are facilities from where DSS personnel can perform essential functions.
7) Achieving the organization’s timely and orderly recovery and reconstitution from an emergency.
8) Ensuring and validating continuity readiness through a dynamic and integrated continuity Test, Training, and Exercise (TT&E) program and operational capability.

G. Security and Privacy Statement

This document is to be treated as confidential. Portions of the plan contain information that raises personal privacy or other concerns, and those portions may be exempt from mandatory disclosure under the Freedom of Information Act (see 5 United States Code §552, 41 Code of Federal Regulations Part 105-60)ii. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the Connecticut Freedom of Information Actiii, and §4-193 Connecticut Personal Data Activ and is not to be released without prior approval of the Commissioner, Department of Social Services to the public or other personnel who do not have a valid “need to know.”

Some of the information in this Plan, if made public, could endanger the privacy of employees. In addition, the disclosure of information in this plan could compromise the security of essential equipment, services, and systems of DSS or otherwise impair its ability to carry out essential functions.

Distribution of the Continuity Plan in whole or part is limited to those personnel who need to know the information in order to successfully implement the plan.

DSS will make the Business Continuity/Disaster Recovery Plan available to appropriate DSS personnel as needed. In addition, copies of the Plan may be distributed to other organizations as necessary to promote information sharing and facilitate a coordinated inter-organization continuity effort.
IV. CONCEPT OF OPERATIONS

A. Phase I: Readiness and Preparedness (Pre-Activation)

The circumstances that may require activation of the Business Continuity/Disaster Recovery Plan will not always be known ahead of time. Therefore, the Department of Social Services will participate in the full spectrum of readiness and preparedness activities to ensure personnel can continue essential functions in an all-hazard / threat environment. DSS readiness activities are divided into two key areas:

Organization Readiness and Preparedness

DSS preparedness incorporates hazard/threat warning systems, which includes those provided to state agencies by the Connecticut Department of Emergency Services and Public Protection (DESPP) and the Division of Emergency Services and Homeland Security (DEMHS).

The Connecticut State Response Framework (SRF) provides guidance under which the state Unified Command would be activated. The Unified Command normally includes Commissioners from affected or involved agencies acting in support of the Governor. The Unified Command is not continually activated but will be activated when an incident appears to be developing or has the potential to develop. DESPP and DEMHS manage this process along with the State Emergency Management Director. The SRF does not specify the DSS Commissioner as a regular member of that Unified Command, but does provide latitude to call upon the DSS Commissioner when the situation dictates.

Staff Readiness and Preparedness

DSS personnel will prepare for a contingency event and plan in advance for what to do in an emergency. This plan will reviewed and updated at least annually but required personnel are expected to familiarize themselves and their teams with the information they require to be successful in the event of an emergency. Additionally, this plan includes provisions for regular tests and exercises to familiarize personnel with the processes to be followed in the event of an emergency situation.

Outside of work, all DSS personnel are encouraged to develop a Family Support Plan to increase personal and family preparedness. The US Department of Homeland Security’s www.ready.gov website provides guidance for developing a Family Support Plan and includes a “Get Ready Now” pamphlet that explains the importance of planning and provides a template that can be tailored to meet family-specific planning requirements.
Agency Day to Day Preparations

Agency leaders are responsible to the personnel within their divisions to remain vigilant and prepared for an incident or contingency situation at any time. Preparations must be made continually. At a division level, DSS must:

1. [ ] DAILY - Remain aware of broadcast news and weather sources
2. [ ] MONTHLY - Ensure call trees are updated with current contact information for employees and contractors, as applicable
3. [ ] MONTHLY - Ensure division email distribution lists are current
4. [ ] MONTHLY - Emergency Operations Center (EOC) members should ensure they have the proper log in credentials for the WebEOC system and are able to access the system
5. [ ] QUARTERLY - Ensure staff are aware of the continuity plan(s) and where to obtain information
6. [ ] QUARTERLY - Ensure personnel understand their roles and responsibilities
7. [ ] ANNUALY - Keep memoranda of understanding up to date with appropriate state agencies (namely Department of Administrative Services)
8. [ ] AS APPLICABLE - Ensure staff are informed of an impending situation (e.g. approaching weather such as a hurricane, snowstorm etc.)

Agency Functions, Service and Process Continuity Priorities

As evidenced in the DSS Influenza Continuity of Operations Plan, DSS has established an exhaustive list of processes carried out by the agency. From that list of processes, the following priorities have been highlighted as those requiring special consideration in the event of a contingency. These processes are the highest priority for DSS.

Each process has an established Recovery Time Objective (RTO). RTO is the amount of time a system or process must be restored following an interruption.

Uninterruptible Functions (RTO of less than 1 Day)

1. Medical and Medical-Related Assistance, including processing Advanced Directives
2. Supplemental Nutrition Assistance Program (SNAP)
3. Cash programs
   a. Temporary Family Assistance (TFA)
   b. Child Support
c. State Administered General Assistance (SAGA)
d. State Supplement Cash Assistance
e. Refugee Assistance

4. Protective Services Crises

5. Conservator Crises

**Critical Functions (RTO greater than 2 but less than 5 Days)**

1. Energy Assistance
2. Housing / Shelter Assistance
3. Child Care Assistance
B. Phase II: Activation

To ensure the ability to attain operational capability at continuity facilities and with minimal disruption to operations, the Department of Social Services will execute activation plans as described in the following sections.

Activation of the Business Continuity / Disaster Recovery Plan will follow the process established in the *Influenza Pandemic Continuity of Operations Plan*. The steps and processes described within this document are a summary of that plan.

**DSS Incident Command Team (ICT)**

DSS has an established Incident Command Team (ICT) hierarchy, pictured below. These are the personnel that will be activated in the event of a contingency situation. The calling list is updated regularly and is emailed to the necessary DSS personnel by the Chief of Staff’s office when it is updated.
ICT Roles and Responsibilities

The Incident Command Team is comprised of 3 elements; the Command Staff, Command Support Staff and General Staff. Their responsibilities are listed in the following section. The roles described are in alignment with the DSS Influenza Pandemic Continuity of Operations Plan.

Command Staff

Incident Commander (IC)

The individual who is responsible for all incident action plans and activities to sustain critical functions and services; these include the development of strategies and tactics before and execution of action plans in the event of an incident, as well as the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site. In the context of the Continuity of Operations Plans, if the Incident Commander is not the Agency Head, they will report to the Agency Head or equivalent agency executive position.

Deputy Commander

A fully qualified individual who, in the absence of a superior, can be delegated the authority to manage a functional operation or perform a specific task. In some cases, a deputy can act as relief for a superior and, therefore, must be fully qualified in the position. Deputies can be assigned to the Incident Commander, Command Support Staff and the Section Chief positions.

Command Support Staff

ECC Liaison Officer

The member of the Incident Command Support Team who provides a liaison function between the Department and the State’s Department of Emergency Management and Homeland Security (DEMHS) Department, especially when DEMHS has elected to activate its Emergency Operations Center (EOC). A close working relationship between the Department and the EOC is required for timely communication and action appropriate to directives received. The EOC Liaison Officer will represent the Department at the EOC and establish ongoing communications and scheduled status reviews with the Department Incident Command.
WEB EOC Liaison

The member of the Incident Command Support Team who provides liaison function among the Department’s Liaison Officer located at the State EOC and Department’s Emergency Command Center (ECC) when activated. A close working relationship between the Department and the EOC is required for timely communication and action appropriate to directives received.

Public Information Officer (PIO)

The member of the Incident Command Support Team who is responsible for drafting and issuing all public announcements, making all press releases and giving all interviews with the communications media relative to the incident and the Department’s action plan to address the situation. The PIO establishes communications with PIOs in other State Agencies and the Governor’s Media Office to convey situation status, progress toward resolving the incident and any actions needed in support of or to address the situation. The PIO works directly with the Incident Commander (IC) and Agency Head on all sensitive communications and may seek advice and counsel from other members of the Command Support Staff on legal or personnel matters and from the Section Chiefs on background relating to the situation and the actions the Department is taking.

Safety Officer

The member of the Incident Command Support Team who is responsible for the physical security of Department personnel and the Public within the custody of the Department; in the context of a public disaster, the Security Officer is to advise on steps to protect staff and residents / clients from unintended or malicious activities that may cause injury or death and to make reports and recommendations to and receive and address recommendations from the State Police, as appropriate to the incident.

Human Resource Officer

The member of the Incident Command Support Team who provides human resources advice and counsel to the Incident Commander; examples of support would include development of plans to assist employees affected by the incident and guidance on union or bargaining unit issues raised by the incident or requirements to respond to the incident. The HRO will have a COOP relationship with Connecticut Department of Administrative Services (DAS) and the Office of Labor Relations (OLR) and may assume some of the Safety Officer responsibilities.
Legal Counsel

The member of the Incident Command Support Team who provides legal counsel to the Incident Commander; examples of support would include advice relative to Department jurisdiction and contractual obligations. The Legal Counsel may also be asked to review any public statements that are to be issued by the Public Information Officer (PIO) or provide opinion and guidance on employee relations based issues or issues that relate to the Department mission and the public. The LC will have a COOP relationship with the Attorney General’s Office, the Office of the Governor and the Judicial Branch.

General Staff

Finance and Administration Section Chief

The Member of the Incident Command General Staff and leader of the Administration Section, which in the context of the Continuity of Operations Program, is responsible for internal processes within the Department, including financial planning and management support to the Incident Commander. Examples of support would include arrangements for emergency funding, financial analysis, financial record keeping, petty cash management and financial reporting. The Section Chief has a COOP relationship with DAS and OPM. The Administration Section sustains or recovers processes to maintain the fiscal integrity of the Department and works closely with the Operations and Logistics Sections to identify requirements and assess available options.

Finance and Administration Section Team Leads

Qualified member of the Incident Command General Staff who reports to the Administration Section Chief; individual responsible for the coordination of the initial action plan execution and recovery efforts for one of the Administration Section Teams. Section Team Leaders are responsible for pre-disaster preparedness, disaster response coordination, disaster recovery and demobilization, and post-disaster corrective actions based on lessons learned for the functions that are part of the normal operational responsibilities of the work group. These Team Leaders often head Branches or Divisions. Section Chiefs will determine the organization appropriate under respective Sections.

Logistics Section Chief

The member of the Incident Command General Staff and leader of the Logistics Section, which in the context of the Continuity of Operations Program, is responsible for the resources and processes needed to sustain or recreate the work environment for Operations and Administration Section functions, including facility, technology, equipment and supplies. The
Logistics Section Chief addresses plant, tool, technology and information security (including HIPAA) requirements for the Incident Command, working closely with the Operations and Administration Sections to identify requirements and assess available options. The *Influenza Pandemic Continuity of Operations Plan* documents two Logistics Chiefs; one from ITS and one from Facilities.

**Logistics Section Team Leads**

These are qualified members of the Incident Command General Staff who reports to the Logistics Section Chief; responsible for the coordination of the initial action plan and recovery efforts of one of the Logistics Section Teams. Section Team Leaders are responsible for pre-disaster preparedness, disaster action plan coordination, disaster recovery and demobilization, and post-disaster corrective actions based on lessons learned for the functions that are part of the normal operational responsibilities of the work group. These Team Leaders often head Branches or Divisions. Section Chiefs will determine the organization appropriate under respective Sections. The *Influenza Pandemic Continuity of Operations Plan* documents two Logistics Chiefs; one from ITS and one from Facilities.

**Operations Section Chief**

The member of the Incident Command General Staff and leader of the Operations Section, who is responsible for the sustenance or recovery of the functions within the department that serve the citizens of the state. The Operations Section Chief directly manages all incident tactical activities and implements the Incident Action Plan (IAP). The Operations Section Chief may have one or more Deputies, who are qualified to assume these responsibilities. This is recommended where multiple shifts are needed, as well as for succession planning.

**Operations Section Team Leads**

Qualified member of the Incident Command General Staff, reporting to the Operations Section Chief; individual responsible for the coordination of the initial action plan and recovery efforts of one of the Operations Section Teams. Section Team Leaders are responsible for pre-disaster preparedness, disaster action plan coordination, disaster recovery and demobilization, and post-disaster corrective actions based on lessons learned for the functions that are part of the normal operational responsibilities of the work group. These Team Leaders often head Branches or Divisions. Section Chiefs will determine the organization appropriate under respective Sections.
Operations Section Field Branch Leads

Qualified member of the Incident Command General Staff, reporting to the Operations Section Chief; individual responsible for the coordination of the initial action plan and recovery efforts of one or all Field Offices. Field Branch Team Leaders are responsible for pre-disaster preparedness, disaster action plan coordination, disaster recovery and demobilization, and post-disaster corrective actions based on lessons learned for the field office functions that are part of the normal operational responsibilities of the work group. These Team Leaders often head Branches or Divisions. Section Chiefs will determine the organization appropriate under respective Sections. The field site locations are listed later in this section.

Planning Section Chief

The member of the Incident Command General Staff and leader of the Planning Section, who is responsible for the development of the COOP document, working closely with the Incident Commander, General Staff (other Section Chiefs) and Command Support Staff to ensure critical functions and their resource requirements are identified, that preparatory actions are taken and that communications information needed to execute the COOP has been captured. In the continuity plan action period, the Planning Section Chief is to serve as a coach to Incident Command and to ensure that regular crisis action plan review sessions are held, that outstanding issues are identified, that appropriate alternatives are considered and that action assignments are clearly distributed. Planning Section Chief may have one or more Deputies, who are qualified to assume these responsibilities. This is recommended where multiple shifts are needed, as well as for succession planning.

Planning Section Team Leaders

Qualified member of the Incident Command General Staff, reporting to the Planning Section Chief; individual responsible for the development of the COOP document, working closely with the Incident Commander, General Staff (other Section Chiefs) and Command Support Staff to ensure critical functions and their resource requirements are identified, that preparatory actions are taken and that communications information needed to execute the COOP has been captured. In the continuity plan action period, the Planning Section Team Leader is to serve as a coach to Incident Commander, Section Chiefs and/or Field Office Leaders to help ensure that regular crisis action plan review sessions are held, that outstanding issues are identified, that appropriate alternatives are considered and that action assignments are clearly distributed. Planning Section Team Leaders may have one or more assistances, which are qualified to assume these responsibilities. This is recommended where multiple shifts are needed, as well as for succession planning.
Field Operations

The DSS Field sites have the opportunity to be uniquely affected by a disaster or continuity situation. Due to their geographically-separated nature, one or more sites may be affected without any impact to other DSS locations.

This document does not supersede any DSS Field Operations Continuity or Contingency Plans developed. Rather it has been informed by Field Operations’ practices. As of March 2018, Field Operations is performing a review and update to their internal Business Continuity Plan.

Decision Process Matrix

Based on the type and severity of the emergency situation, the Continuity Plan may be activated when the DSS Commissioner or their appointed successor determines that a Disaster Declaration is in order.

Continuity Plan activation is a scenario-driven process that allows for flexible and scalable responses to the full spectrum of hazards and threats that could disrupt operations with or without warning and during work or non-work hours. To aid in their decision-making process, key personnel will use the following decision matrix to determine the appropriate response. The answers provided to these questions will help determine:

1. Does the event have the ability to cause harm to DSS personnel?
2. Can the effects of an event be mitigated in advance?
3. Will DSS offices be directly affected? Should they remain open?
4. It is safe for DSS personnel report to their normal work locations or should they be deployed elsewhere?
5. How prepared are other DSS location to accept an influx of staff?
6. Will information technology be affected and what can be done to mitigate any affects ahead of time?

<table>
<thead>
<tr>
<th>Event with Warning</th>
<th>During Work Hours</th>
<th>Non-Work Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>▪ Is the threat aimed at a DSS facility or surrounding area?</td>
<td>▪ Is the threat aimed at a DSS facility or surrounding area?</td>
</tr>
<tr>
<td></td>
<td>▪ Is the threat aimed at DSS personnel?</td>
<td>▪ Is the threat aimed at DSS personnel?</td>
</tr>
<tr>
<td></td>
<td>▪ Are employees unsafe remaining in the facility and/or area?</td>
<td>▪ Who should be notified of the threat?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Is it safe for employees to return to work the next day?</td>
</tr>
<tr>
<td>Event without Warning</td>
<td>Are DSS facility(ies) affected?</td>
<td>Are DSS facility(ies) affected?</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
</tbody>
</table>

As the decision authority, the DSS Commissioner will be kept informed of the threat environment using all available means, including regional notification systems, local operations, State and local reporting channels and news media. The Commissioner will evaluate all available information relating to:

1. Direction and guidance from higher authorities
2. The health and safety of personnel
3. The ability to execute essential functions
4. Changes in threat advisories
5. Intelligence reports
6. The potential or actual effects on communications systems, information systems, office facilities, and other vital equipment
7. The expected duration of the emergency situation

**Alert and Notification Procedures**

In the event normal operations are interrupted or an incident appears to be imminent, DSS will take the following steps to communicate the organization’s operating status with all staff:

1. In the event of a critical IT issue or emergency, the first indications may be identified by IT staff either through their own observation of the system or by a system alert via electronic means. In this case, the IT staff will initiate their Business Continuity procedures which will include contacting the appropriate DSS Leadership, i.e. the Commissioner and the Chief of Staff for their situational awareness.

2. Each division or business unit will activate their call trees as identified and follow their procedures.

3. The State of Connecticut employs the CT Alert Emergency Notification System (ENS) to all residents. These are text messages that may be sent out should there be some sort of incident or event. Residents must sign up for these alerts in order to begin receiving them.
4. DSS personnel, including contractor personnel can also use the DESPP or DEMHS web sites for up to date information on office closures. Personnel should navigate their web browsers to:

www.ct.gov/despp or www.ct.gov/demhs

Once on either of the sites, look for the red “State Offices: Early Release/Late Openings/Closures” box on the left side of the front page. Please note that these sites may not

5. Additionally, DSS has a staff alert hotline which is updated in concert with the DESPP and DEMHS web sites. Those numbers are:

DSS STAFF ALERT HOT LINE

REDACTED

6. Finally, local broadcast television and radio stations may also have information for local state facility closures. Please note that different areas within Connecticut may have different broadcast resources so information may not be disseminated evenly or quickly following a contingency situation.

Upon the decision to activate the Continuity Plan, DSS personnel will be notified along with affected and interdependent entities (e.g. vendors, contractors, etc.) with information regarding continuity activation status, operational and communications status, and the anticipated duration. These entities include:

Communications

The communications requirements are documented in the Influenza Pandemic Continuity of Operations Plan and should be consulted. The following information provides basic guidance and does not supersede other established procedures.

Per the Connecticut State Response Framework when information of a potential incident exists, such as in the case of an approaching weather system for example, DESPP/DEMHS will provide state agencies with situational awareness to allow for activation of the continuity plan. Should an incident or event occur without warning, DESPP/DEMHS will inform the Unified Command of the situation and required responses through conference calls. Agencies will enact their continuity plans as required.
As a contingency situation continues to develop, the Department of Social Services will require the collection and dissemination of critical information internally and externally. While specific incidents may create additional or specialized reporting requirements, the following table lists examples of the information that should be collected and reported regardless of incident type.

**Internal Communications**

The *Influenza Pandemic Operations Plan* has established email as the preferred method of internal communication when it is available as it provides the widest dissemination in the shortest amount of time. Telephone will be the next preferred method.

The table below provides specific examples of internal DSS communications that are required during an incident.
### External Communications

External communications MUST be coordinated with the DSS Office of Public Affairs, especially those released to the general public. These processes are detailed in the *Influenza Pandemic Continuity of Operations Plan*. The following information provides basic guidance and does not supersede other established procedures.
The following guidance has been documented in the *Influenza Pandemic Continuity of Operations Plan* for the dissemination of external communications.

1. External messages must be coordinated with all necessary DSS parties before being released.

2. The Office of Public Affairs must communicate any external messages internally to DSS personnel to ensure consistency of message. This will also pre-emptively educate those DSS personnel to answer any questions they may receive over the phone with Connecticut residents.

3. Office of Public Affairs will assist specific field offices or divisions should the need arise.

4. The Office of Public Affairs will coordinate with the SEOC and Governor’s Communication Office as the situation warrants.

5. Information will be posted on critical agency web sites.

6. Voice information (a.k.a. podcasts) will be posted on the DSS main web site to provide information to those who are unable to read the information.

7. The dedicated toll-free information line will be activated to provide ‘need to know’ information to DSS clients/applicants. This toll-free line will allow the option for personnel to speak to a live representative or provide an option to leave a voicemail.
8. TDD/TYY capability will be enabled and publicized

**Emergency Command Center (ECC)**

If the Continuity Plan is activated, the Incident Commander may determine the activation of the Emergency Command Center is also warranted.

<table>
<thead>
<tr>
<th>Emergency Command Center Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone</strong></td>
</tr>
<tr>
<td>REDACTED</td>
</tr>
</tbody>
</table>

**Relocation Operations**

Once the Continuity Plan is activated and personnel are notified, essential DSS continuity personnel (i.e. Level 1 Employees) may be required to deploy/relocate to the continuity facility(ies) to perform the essential functions and other continuity-related tasks. Eligible locations for relocation will be determined ahead of time and may include DSS field sites or other state agencies, as required. Certain functions will only relocate to eligible DSS facilities due to the sensitive nature of the data they utilize in the performance of the business function. These limitations will be highlighted in the functional annexes of this document.

**Relocation – During Work Hours**

Emergency procedures during work hours with or without a warning will be implemented as follows:

- Continuity personnel, if applicable, will depart to the designated continuity facility from the primary operating facility or current location using privately owned vehicles.
- Non-continuity personnel present at the primary operating facility or another location will receive instructions from their supervisors. In most scenarios, non-continuity personnel will be directed to proceed to their homes or other DSS facilities, if appropriate, to wait for further guidance.
- At the time of notification, if available, information will be provided regarding safety precautions and routes to use when leaving the primary operating facility.

**Relocation – During Non-Work Hours**

Emergency procedures during non-working hours with or without a warning will be implemented as follows:

- If warranted by the situation, designated personnel will deploy to the designated continuity facility from their current location using privately owned vehicles.
Business Continuity/Disaster Recovery Plan
VERSION: 1.0

- Continuity personnel will depart to the assigned continuity facility from their current location using privately owned vehicles.
- Non-continuity personnel will remain at their residence or other designated facility to wait for further instructions.

Non-continuity personnel may be required to replace or augment continuity personnel during activation. These activities will be coordinated by each division’s leadership with the replacement staff on a case-by-case basis. Non-continuity personnel will remain available to replace or augment continuity personnel, as required.

In the event of an activation of the Continuity Plan, DSS may need to procure necessary personnel, equipment, and supplies that are not already in place for continuity operations on an emergency basis. This process will be coordinated with the Logistics Section Chiefs, who are members of Incident Command Team and their respective teams.

Field Operations Relocation

The twelve regional DSS field offices have unique challenges when office relocation is required. As of March 2018, Field Operations is in the process of documenting its Continuity Operations Plan as a number of factors have driven the requirement to do so. Determining the Relocation of a DSS Field site is currently a highly manual process requiring a great deal of coordination.

There are several considerations to be weighed when relocation is a possibility.

1. **No Manual Processes** - The majority of critical Field Office functions are IT-based, meaning there is no manual backup to the process. Should an office lose IT capabilities (i.e. connection to IMPACT), they will be rendered inoperative until that connection is restored.

2. **Distance Restrictions** - Depending on which site(s) need to be relocated will determine which DSS employee can be deployed. Per their collective bargaining arrangement DSS employees are limited to a 50 mile round trip commute from their place of residence to an alternate site. Each redeployment decision must be made individually. Due to this factor, it is possible that the majority of a field site staff may go to one location while other(s) may be assigned elsewhere.

3. **Alternate Site Constraints** – Several DSS Field sites have restrictions to the number of personnel they are able to host. This is due to combination of the number of IT resources, phones, seating and in the case of the Waterbury field office, the availability of parking. Other restrictions exist and require the input of the Field Operations Branch Leader, a member of the Incident Command Team.

Should a relocation of a DSS field site be required, Field Operations will generally follow the
relocation guidance below. However, please note that all the information previously discussed must be factored.

<table>
<thead>
<tr>
<th>Affected Office</th>
<th>May Relocate to</th>
</tr>
</thead>
<tbody>
<tr>
<td>REDACTED</td>
<td>REDACTED</td>
</tr>
</tbody>
</table>
C. Phase III: Continuity Operations

Upon activation of the Continuity Plan, DSS will continue to operate at its primary operating facility at 55 Farmington Ave, Hartford, CT and field locations until ordered to cease operations by the Incident Commander (IC), designated successor or other State of Connecticut authorities (e.g. DESPP or DEMHS). At that time, essential functions will transfer to the continuity facility(ies) as is operationally feasible.

The *Influenza Pandemic Continuity of Operations Plan* provides guidance on the processes to follow during a continuity event including those where relocation is required for some or all of DSS. This guidance includes a division by division determination of the required processes, staffing requirements and other resource requirements.

Depending on the situation, it may be necessary for DSS to dispatch an ‘advance team’ of information technology personnel to ensure the required IT resources are in place and functioning to support continuity operations. This advance team will be first to arrive at the continuity facility to prepare the site for the arrival of other continuity personnel. Upon arrival at the continuity facility, the advance team, along with local facility personnel will:

- Ensure infrastructure systems, such as power and heating, ventilating, and air conditioning are functional

- Establish the necessary data connections including critical applications, file servers, telephones printers, etc. Specific systems and priorities are listed in Annex A of this document.
D. Phase IV: Reconstitution Operations

Once an incident has subsided, State of Connecticut authorities (e.g. DESPP, DEMHS or others) along with the Commissioner will determine when it is appropriate to return to regular operations. State authorities will initiate and coordinate operations to salvage, restore, and recover the DSS facility at 55 Farmington Ave, Hartford, CT after receiving approval from the appropriate Federal, State and local law enforcement and emergency services.

- The Commissioner will appoint a Reconstitution Manager for all phases of the reconstitution process
- Each DSS Division and Business Unit will designate a reconstitution point-of-contact (POC) to work with the Reconstitution Team and to update office personnel on developments regarding reconstitution.

During continuity operations, the Commissioner should be regularly apprised of the status of the primary operating facility affected by the event by state agencies and DSS personnel. Upon obtaining the status of the facility, DSS will determine how much time is needed to repair the primary operating facility and/or acquire a new facility. This determination is made in conjunction with appropriate state agencies, including but not limited to Department of Administrative Services and other necessary state agencies and boards. Plan development and maintenance

The Department of Social Services is responsible for maintaining this Business Continuity/Disaster Recovery Plan. This Plan, essential functions, and supporting activities, will be reviewed by the divisions which appear in Appendix X and updated annually from the date of publication as part of the maintenance of continuity plans and procedures. In addition, the plan will be updated or modified when there are significant organizational, procedural changes, or other events that impact continuity.

V. IDENTIFICATION OF ESSENTIAL FUNCTIONS

The identification of essential functions is documented in great detail in the DSS Influenza Pandemic Continuity of Operations Plan and should be referenced should the activation of this plan become necessary. The Influenza Pandemic Continuity of Operations Plan provides a comprehensive listing of all agency functions, priorities as well as personnel required. These essential functions should be reviewed at least annually and this plan should be updated any time an essential function is added, altered or deleted.
VI. IDENTIFICATION OF CONTINUITY PERSONNEL

In order for DSS to continue its essential functions, certain positions and personnel will be determined to be necessary during a Business Continuity / Disaster Recovery plan activation. The DSS *Influenza Pandemic Continuity of Operations Plan* provides a detailed list of the Level 1 and Level 2 personnel required to perform essential and non-essential functions for across all DSS Divisions and Field locations.

These personnel requirements should be reviewed at least annually and this plan should be updated any time a change is necessitated.

VII. TEST, TRAINING, AND EXERCISES PROGRAM

This plan is based heavily on the processes and priorities detailed in the *Influenza Pandemic Continuity of Operations Plan* which is routinely tested across all elements of DSS. It is critical that the Business Continuity and Disaster Recovery plan is regularly tested and exercised. This is to ensure it flows properly, identifies the right personnel resources and also to identify areas that must be updated within the plan. This process will ensure personnel are properly trained on the necessary steps. Feedback (i.e. lessons learned) from participants and business process owners must be incorporated into this process.

There are two different types of tests that can be performed. Each type validates a different set of criteria and requires a varying level of personnel support.

- **Table-top exercise:** A table-top is a structured walk through of the Business Continuity Plan. It generally requires a limited level of effort as it is intended to familiarize participants with the contents and procedures within the plan, without going through the physical motions of recovering systems. A well-planned and executed table top will build confidence within the organization as participants will help validate their abilities to locate necessary procedures and to perform critical functions in a recovery situation.

- **Functional exercise:** A functional exercise allows personnel to validate the plan and readiness by performing their duties in an operational environment. These can be scenario-driven; such as simulating a disaster at a DSS facility requiring the organization to reconstitute operations at an alternate location. They can also be scaled to exercise specific portions or functions within the business, such as only testing a particular division, team or process. They may also be full scale, involving all divisions and business units as well as outside agencies and even commercial partners.
The Agency may choose to perform these exercises as announced or unannounced, though it is not recommended to perform an unannounced exercise unless the plan has been tested several times.

Annex A: Information Technology Services (ITS)

A.1 – A.6

Redacted for the purpose of this distribution

A.7 Roles and Responsibilities

Pre-Disaster Responsibilities

General Division Responsibilities

1. Maintain a copy of the personnel contact list in a location which is available off-line. Ensure it is always up to date. This includes maintaining the contact information of contractor personnel, when applicable.
2. Participate in walkthroughs of the Business Continuity/Disaster Recovery Plan and ensure every team member is thoroughly familiar with the plan and the process. This should be accomplished at least annually, but more frequently is recommended.
3. Develop and implement processes and procedures that will enhance the readiness of the department in a disaster recovery.

Team Leader

1. Provide overall leadership in the development and the implementation of the Business Continuity/Disaster Recovery Plan
2. Implement and test the Business Continuity/Disaster Recovery Plan
3. Establish a team notification plan and predetermined meeting location for disaster assessment
4. Ensure all team personnel are familiar with the notification procedures and the Business Continuity/Disaster Recovery Plan
5. Participate in the periodic testing of the Business Continuity/Disaster Recovery Plan
6. Preview test plans and test results. Ensure the plan is updated after each test, as appropriate
7. Document the vital records inventory. Keep this document updated and stored off site
Team Members

1. Perform daily backups of all critical IT systems and coordinate off-site media rotation.
2. Develop, validate, and document the recovery procedures for critical applications.
3. Document and maintain current LAN diagrams and network recovery procedures.
4. Collect and store off-site all vital records and procedures required for BC/DRP.
5. Periodically test recovery procedures of IT critical systems.
6. Review and analyze test results and update plan and procedures as necessary.
7. Cross train team members in recovery of systems, database, and applications.
8. Work with IT personnel to identify/develop interim manual procedures, as appropriate.
9. Contact software vendors to make arrangements for emergency response and recovery.
10. Know, understand, and maintain the IT Disaster Recovery plan for all CVH supported systems.

Disaster Responsibilities

Team Leader

1. Alert all team members when notified of the potential disaster.
2. Once a disaster is declared, initiate the telephone call chain within the Business Unit.
3. Keep close communication with the Command Center.
4. When the temporary office spaces are ready, notify team members and provide direction to the alternate work site.
5. Review the responsibilities and emergency tasks.
6. Modify and assign priorities to the tasks based on the current demands on the Business Unit.
7. Assign members to the emergency tasks.
8. Meet with Team Members to determine critical path and prioritize business functions.

Team Members

1. Report to the alternate work location when notified to do so.
2. Coordinate with the Administration Team in the retrieval of vital records from off-site storage.
3. Review the Business Unit recovery procedures with the team leader before executing the procedures.
4. Take a record inventory to determine if any of the vital records are salvageable.
**Post-Disaster Responsibilities**

1. Assess the effectiveness of the department Business Continuity Teams.
3. Revise/update existing procedures.

A.8 – A.17

Redacted for the purpose of this distribution

**GLOSSARY**

*Activation* – Once a continuity of operations plan has been implemented, whether in whole or in part, it is considered “activated.”

*All-Hazards* – The spectrum of all types of hazards including accidents, technological events, natural disasters, terrorist attacks, warfare, and chemical, biological including pandemic influenza, radiological, nuclear, or explosive events.

*Alternate Facilities* – Locations, other than the primary facility, used to carry out essential functions, particularly in a continuity event. “Alternate facilities” refers to not only other locations, but also nontraditional options such as working at home (teleworking), telecommuting, and mobile-office concepts.

*Business Impact Analysis (BIA)* – A method of identifying the effects of failing to perform a function or requirement.

*Communications* – Voice, video, and data capabilities that enable the leadership and staff to conduct the mission essential functions of the organization. Robust communications help ensure that the leadership receives coordinated, integrated policy and operational advice and recommendations and will provide the ability for governments and the private sector to communicate internally and with other entities (including with other Federal agencies, State, territorial, tribal, and local governments, and the private sector) as necessary to perform their Mission Essential Functions (MEFs).

*Continuity* – An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event.

*Continuity of Operations* – An effort to ensure they can continue to perform their Mission Essential Functions and Primary Mission Essential Functions during a wide range of emergencies,
including localized acts of nature, accidents, and technological or attack-related emergencies.

**Continuity Event** – Any event that causes an agency to relocate its operations to an alternate or other continuity site to assure continuance of its essential functions.

**Continuity Personnel** – Those personnel, both senior and core, who provide the leadership advice, recommendations, and functional support necessary to continue essential operations. Per Executive Order 65, dated March 21, 2018, essential employees are to be referred to as “Level 1” employees. Non-essential employees are to be referred to as “Level 2.”

**Essential Functions** – The critical activities performed by organizations, especially after a disruption of normal activities. There are three categories of essential functions: National Essential Functions, Primary Mission Essential Functions, and Mission Essential Functions.

**Facilities** – Locations where an organization’s leadership and staff operate. Leadership and staff may be co-located in one facility or dispersed across many locations and connected by communications systems. Facilities must be able to provide staff with survivable protection and must enable continued and endurable operations.

**PRIMARY** – Data Center

**Leadership** – The senior decision makers who have been elected (e.g., the President, State governors) or designated to head a branch of government or other organization.

**Mission Essential Functions** – The limited set of agency-level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.

**Primary Operating Facility** – The site of an organization’s normal, day-to-day operations; the location where the employee usually goes to work.

**Reconstitution** – The process by which surviving and/or replacement organization personnel resume normal operations from the original or replacement primary operating facility.

**Risk Analysis** – The process by which risks are identified and evaluated.

**Risk Assessment** – The identification and assessment of hazards.

**Risk Management** – The process of identifying, controlling, and minimizing the impact of events whose consequences are or may be unknown, or events that are fraught with uncertainty.

**SECONDARY** – Data Center

**Telework** – The ability to work at a location other than the official duty station to perform work or emergency duties. This may include, but is not limited to, using portable computers,
personal computers, high-speed telecommunications links, and mobile communications devices.

**Testing, Training, and Exercises** – Measures to ensure that an agency’s continuity plan is capable of supporting the continued execution of the agency’s essential functions throughout the duration of a continuity situation.

**REFERENCES**

5. Executive Order 65, dated March 21, 2018 modified the terminology “Essential Employee” and Non-Essential Employees” to be referred to as Level 1 and Level 2 employees respectively. [http://portal.ct.gov/-/media/BE976D35270340FC952DC39BC2D39406.pdf](http://portal.ct.gov/-/media/BE976D35270340FC952DC39BC2D39406.pdf)