





Secure One HHS

System-level Contingency Plan Template

Current Date

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Table of Contents

Table of Contents **1**
RECORD OF CHANGES **2**
1. INTRODUCTION **3**
1.1 PURPOSE 3
1.2 APPLICABILITY 3
1.3 SCOPE 3
1.3.1 Planning Principles 3
1.4 REFERENCES/REQUIREMENTS 4
2. CONCEPT OF OPERATIONS **6**
2.1 SYSTEM DESCRIPTION AND ARCHITECTURE 6
2.2 LINE OF SUCCESSION 6
2.3 RESPONSIBILITIES 6
3. NOTIFICATION AND ACTIVATION PHASE **7**
4. RECOVERY OPERATIONS **9**
5. RETURN TO NORMAL OPERATIONS **10**
Original or New Site Restoration 10
5.1 CONCURRENT PROCESSING 10
5.2 PLAN DEACTIVATION 10
6. PLAN APPENDICES **11**

RECORD OF CHANGES

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

1. INTRODUCTION

1.1 PURPOSE

This *{system name}* Contingency Plan establishes procedures to recover the *{system name}* following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Notification/Activation phase*** to detect and assess damage and to activate the plan
  - ***Recovery phase*** to restore temporary IT operations and recover damage done to the original system
  - ***Reconstitution phase*** to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out *{system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated OPDIV personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other OPDIV staff who will participate in the contingency planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 APPLICABILITY

The *{system name}* Contingency Plan applies to the functions, operations, and resources necessary to restore and resume OPDIV*'s {system name}* operations as it is installed at {*primary location name, City, State}*. The *{system name}* Contingency Plan applies to OPDIV and all other persons associated with *{system name}* as identified under Section 2.3, Responsibilities.

The *{system name}* Contingency Plan is supported by {*plan name},* which provides the {*purpose of plan}.* Procedures outlined in this plan are coordinated with and support the {*plan name},* which provides {*purpose of plan}.*

1.3 SCOPE

1.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles.

- OPDIV*'s* facility in {*City, State},* is inaccessible; therefore, OPDIV is unable to perform *{system name}* processing for the Department.

- A valid contract exists with the {*alternate site}* that designates that site in {*City, State},* as the OPDIV's alternate operating facility.
  - OPDIV will use the *alternate site* building and IT resources to *recover {system name} functionality* during an emergency situation that prevents access to the *original facility*.

- The designated computer system at the *alternate site* has been configured to begin processing *{system name}* information.
- The {*alternate site*} will be used to continue *{system name}* recovery and processing throughout the period of disruption, until the return to normal operations.

1.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan.

- The *{system name}* is inoperable at the OPDIV computer center and cannot be recovered within *48 hours.*
- Key *{system name}* personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the *{system name}* Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Computer center equipment, including components supporting {*system name}*, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- *{System name}* hardware and software at the OPDIV {*original site}* are unavailable for at least *48 hours.*
- Current backups of the application software and data are intact and available at the {*offsite storage facility}.*
- The equipment, connections, and capabilities required to operate *{system name}* are available at the {*alternate site*} in {*City, State*}.
- Service agreements are maintained with *{system name}* hardware, software, and communications providers to support the emergency system recovery.

The *{system name}* Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations.** The Business Resumption Plan (BRP) and Continuity of Operations Plan (COOP) are appended to the plan.
- **Emergency evacuation of personnel.** The Occupant Evacuation Plan (OEP) is appended to the plan.

Any additional constraints should be added to this list.

1.4 REFERENCES/REQUIREMENTS

This *{system name}* Contingency Plan complies with the OPDIV IT Contingency Planning Policy as follows:

> *The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be*

trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The *{system name}* Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, November 2000
- Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations*, July 1999
- Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*, October 1998
- PDD 63, *Critical Infrastructure Protection*, May 1998
- Federal Emergency Management Agency (FEMA), *The Federal Response Plan (FRP)*, April 1999
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000
- *{Any other applicable federal policies should be added.}*
- *{Any other applicable departmental policies should be added.}*

2. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

{Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.}

2.2 LINE OF SUCCESSION

OPDIV sets forth an order of succession, in coordination with the order set forth by the Department to ensure that decision-making authority for the *{system name}* Contingency Plan is uninterrupted. The Chief Information Officer (CIO), {OPDIV}, is responsible for ensuring the safety of personnel and the execution of procedures documented within this *{system name}* Contingency Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority. {*Continue description of succession as applicable.}*

2.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering *{system name}* operations. The *{team name}* is responsible for recovery of the *{system name}* computer environment and all applications. Members of the *team name* include personnel who are also responsible for the daily operations and maintenance of *{system name}*. The *team leader title* directs the *{team name}.*

{Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation.}

The relationships of the team leaders involved in *system* recovery and their member teams are illustrated in Figure XX below.
{Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.}

{Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.}

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {*system name*}. Based on the assessment of the event, the plan may be activated by the {*Contingency Planning Coordinator*}. In an emergency, {OPDIV's} top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the {*Contingency Planning Coordinator}*. All known information must be relayed to the {*Contingency Planning Coordinator}.*
- The {*systems manager*} is to contact the {*Damage Assessment Team Leader*} and inform them of the event. The {*Contingency Planning Coordinator*} is to instruct the Team Leader to begin assessment procedures.
- The {*Damage Assessment Team Leader*} is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the {*Damage Assessment Team*} is to follow the outline below:
  - Damage Assessment Procedures:
    - *{Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.}*
    - Upon notification from the *Contingency Planning Coordinator,* the Damage Assessment Team Leader is to …
    - The Damage Assessment Team is to ….
  - Alternate Assessment Procedures:
    - Upon notification from the *Contingency Planning Coordinator,* the {*Damage Assessment Team Leader* is to …}
    - *{The Damage Assessment Team* is to …. }
      - When damage assessment has been completed, the {*Damage Assessment Team Leader*} is to notify the {*Contingency Planning Coordinator*} of the results.
      - The {*Contingency Planning Coordinator*} is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
      - Based on assessment results, the {*Contingency Planning Coordinator*} is to notify assessment results to civil emergency personnel (e.g., police or fire department) as appropriate.
- The Contingency Plan is to be activated if one or more of the following criteria are met:
  - *{system name}* will be unavailable for more than 48 hours
  - *{Facility is damaged and will be unavailable for more than 24 hours*
  - *Other criteria, as appropriate}*

- If the plan is to be activated, the {*Contingency Planning Coordinator}* is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the {*Contingency Planning Coordinator*}, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The {*Contingency Planning Coordinator*} is to notify the {*off-site storage facility}* that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the *alternate site.*
- The {*Contingency Planning Coordinator*} is to notify the {*alternate site*} that a contingency event has been declared and to prepare the facility for the {*Organization's}* arrival.
- The {*Contingency Planning Coordinator}* is to notify remaining personnel (via notification procedures) on the general status of the incident.

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the *{system name}* at the *alternate site.* Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. *State the first recovery objective as determined by the Business Impact Assessment (BIA). {For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.}*

- *{team name}*
  - *Team* Recovery *Procedures*
- *{team name}*
  - *Team* Recovery *Procedures*
- *{team name}*
  - *Team* Recovery *Procedures*

Recovery Goal. {*State the second recovery objective as determined by the BIA. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.}*

- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

Recovery Goal. {*State the remaining recovery objectives (as determined by the BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.}*

5. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring *{system name}* operations at the {*OPDIV's*} original or new site. When the computer center at the original or new site has been restored, *{system name}* operations at the {*alternate site*} must be transitioned back. The goal is to provide a seamless transition of operations from the {*alternate site*} to the computer center.

Original or New Site Restoration

{Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested}.

- *{team name}*
  - *Team Resumption* Procedures
- *{team name}*
  - *Team Resumption Procedures*

5.1 CONCURRENT PROCESSING

{Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.}

- *{team name}*
  - *Team Resumption Procedures*
- *{team name}*
  - *Team Resumption Procedures*

5.2 PLAN DEACTIVATION

{Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site. }

- *{team name}*
  - *Team Testing Procedures*
- *{team name}*
  - *Team Testing Procedures*

6. PLAN APPENDICES

{The appendices included should be based on system and plan requirements.

Personnel Contact List

Vendor Contact List

Equipment and Specifications

Service Level Agreements and Memorandums of Understanding

IT Standard Operating Procedures

Business Impact Analysis

Related Contingency Plans

Emergency Management Plan

Occupant Evacuation Plan

Continuity of Operations Plan}