IT Contingency and Disaster Recovery Plan For

{System Name}
System/Application

U.S. Department of Homeland Security
{Component Name}

Version 1.0

Date: {Month & Year}

DEPARTMENT OF HOMELAND SECURITY

This page intentionally left blank

1 SIGNATURE PAGE

Approval

This Information Technology (IT) Contingency and Disaster Recovery Plan was prepared in accordance with Federal guidance and aligns with the National Institute of Standards and Technology (NIST) Special Publication 800-34, *IT Contingency Planning Guide for Information Technology Systems*, Appendix A. This IT Contingency Plan has been reviewed and meets the requirements for the general support system or major application contingency requirements and complies with internal policies.

Due to the content of this document, this IT Contingency Plan is marked with the appropriate security label: "*For Official Use Only.*"

Submitted by: _____ Date: _____

{Typed name of IT Contingency Planning Coordinator, or designated System Owner}

{Title of System Owner}

I hereby approve this IT Contingency Plan, which is provided for the {system name} system and describes how the continuity of this system will be performed in the event of an emergency or disaster that prevents normal operations.

Approved by: _____ Date: _____

{Typed Name}

Chief Information Officer

This page intentionally left blank

2 RECORD OF CHANGES

Modifications made to this plan are as follows:

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

This page intentionally left blank

CONTENTS

3 INTRODUCTION

3.1 Purpose

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

- In an emergency, the *Customs and Border Protection (CBP)* top priority and objective is to preserve the health and safety of its staff.
- 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 *CBP* personnel and provide guidance for recovering {*system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other *CBP* 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.

3.2 Applicability

The {*system name}* IT Contingency Plan applies to the functions, operations, and resources necessary to restore and resume *CBP* {*system name}* operations as it is installed at {*primary location name, city, state}*. The {*system name}* IT Contingency Plan applies to *CBP* and all other persons associated with *{system name}* as identified under Section **Error! Reference source not found.**, Responsibilities.

The *{system name}* IT Contingency Plan is supported by {*plan name, i.e. DHS HQ COOP Plan, DHS CIO COOP Implementation Plan},* which provides the {*purpose of plan}*. Procedures outlined in this plan are coordinated with and support the {*plan name}*, which provides {*purpose of plan}*.

3.3 Scope

3.3.1 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.

- The CBP facility in *City, State*, is inaccessible; therefore, CBP is unable to perform {*system name*} processing for the {*Department, i.e. DHS Component and office*}.

- A valid contract or plan exists with an alternate site that designates that site in *City, State*, as the alternate operating facility for CBP.

  – CBP 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.

3.3.2 Assumptions

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

- The {*system name*} is inoperable at the CBP computer center and cannot be recovered within {48} hours.
- Key {*system name*} personnel have been identified and trained in their IT contingency planning roles; they are available to activate the {*system name}* IT Contingency Plan.
- Preventive controls (e.g., generators, uninterruptible power supply (UPS), environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are, or may not be fully operational at the time of the disaster. Existing preventive controls are documented and are provided as an attachment to this plan.
- {*System name*} hardware and software at the CBP 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*} IT 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 (COOP) Plans are appended to this plan.
- **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) is appended to this plan. As stated, this appended plan addresses occupant emergencies and is not the IT Contingency Plan.
- *{Any additional constraints should be added to this list and appended to this plan}*.

3.4 References/Requirements

This {*system name*} IT Contingency Plan complies with the CBP IT contingency planning policy as follows:

The CBP shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption. The procedures for execution of such a capability shall be documented in a formal IT 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.

This {*system name*} IT Contingency Plan complies with the following federal and departmental policies and guidance:

- The Privacy Act of 1974.
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 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.
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, November 2000.
- E-Government Act (Public Law 107-347), Title III, "Federal Information Security Management Act," December 2002.
- Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, June 15, 2004.
- {Any other applicable federal or local policies should be added.}

4 CONCEPT OF OPERATIONS

4.1 System Description And Architecture

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

4.2 Order Of Succession

The *CBP* 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*} IT Contingency Plan is uninterrupted. The *{Facility Manager or Security Officer}*, CBP is responsible for ensuring the safety of personnel. The *{System Owner, IT Contingency Plan Coordinator and/or delegated personnel}* is responsible for execution of procedures documented within this {*system name*} IT Contingency Plan. If the {*System Owner / IT Contingency Plan Coordinator}* is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the person delegated responsibility by the system owner shall function as that authority. Documented orders of succession and/or delegations are attached to this plan for reference.

{Continue description of succession as applicable}.

4.3 Responsibilities

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

The IT 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, with information/narrative similar to the above, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation. Following are teams that should be considered for inclusion, and some sample descriptions for various teams and personnel that should be modified and included as needed}.*

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}.

Senior Management Official/CIO/System Owner/IT Contingency Planning Coordinator

This individual is a member of the Senior Management and has responsibility to the Executive Management for all facets of Contingency and Disaster Recovery planning, exercises, and actual recovery efforts.

- **Pre-disaster:**
  - Approve the plan
  - Ensure the plan is maintained
  - Ensure training is conducted
  - Authorize periodic plan testing exercises
  - Support the Team Leader of the Contingency/Emergency Management Team and all other participants prior to and during scheduled and unscheduled exercises/tests of the plan
- **Post-Disaster:**
  - Declaration of a disaster
  - Authorize travel and housing arrangements for team members
  - Authorize expenditures through the Administration Team
  - Manage and monitor the overall recovery process
  - Periodically advise Senior Staff, Customers, and Media & Press Relations personnel of the status
  - Support the Team Leader of the Contingency/Emergency Management Team and all other participants during debilitating conditions/situations

Contingency/Emergency Management Team

{The functionality provided below may also be relevant to a team with the name of:

Alternate Site Recovery Coordination Team}

This team is responsible for managing the total recovery effort, ensuring other teams and personnel perform all detailed checklists, providing a "Command Center" for coordination and overall communications, ensuring that activities are accomplished among all teams within planned time frames and assist in resolving problems that arise. This team is activated by the **Senior Management Official/CIO/System Owner/IT Contingency Planning Coordinator.** All other teams report directly to the **Contingency/Emergency Management Team.** Specific duties are:

Team Leader

- **Pre-disaster**:
    - Maintain and update the plan as needed or scheduled but not less than annually
    - Distribute copies of plan to team members
    - Coordinate Testing as needed or scheduled but not less than annually
    - Train team members
- **Post-disaster:**
    - Establish Command Center for recovery operations
    - Assist in damage assessment
    - Perform initial notification of disaster declaration to members of the Contingency/Emergency Management Team
    - Coordinate activities of the recovery teams
    - Notify alternate site of activation (pending or real)
    - Notify Team Leaders for other Teams of disaster declaration
    - Authorize the Administration Team to make the necessary travel and hotel accommodations for recovery team members
    - Periodically report to Senior Management Official/CIO/System Owner/IT Contingency Planning Coordinator details and status of recovery efforts

Team Members:

- **Pre-disaster**:
    - Assist the Team Leader as directed
    - Participate in contingency exercises
    - Understand role and responsibilities within the Contingency Plan and of the team
- **Post-disaster:**
    - Perform command center functions
    - Maintain a record of all communications using the provided log forms

Damage Assessment Team:

Team is responsible for damage assessment of the computer facilities as quickly as possible following an incident and reporting the level of damage to the Contingency/Emergency Management Team. Also, provides assistance as possible in the cleanup and repair of the facility. Specifically, the team is responsible for:

- **Pre-disaster**:
    - Understand role and responsibilities within this plan

- Work closely to reduce possibilities for contingencies and disasters
- Train employees in emergency preparedness
- Participate in contingency exercises
- Know the procedures to be followed

- **Post-disaster:**
  - Determine accessibility to facility, building, offices, and work areas/stations
  - Assess extent of damage to the system and computer center
  - Assess need and/or adequacy of physical security/guards
  - Estimate time to recover primary facility and system
  - Identify salvageable hardware
  - Apprise the Contingency/Emergency Management Team on the extent of damages, estimated recovery time, need for physical security, and details of salvageable equipment
  - Maintain a log/record of all salvageable equipment
  - Coordinate with vendors/suppliers in restoring, repairing or replacing equipment not under the purview of another contingency/disaster recovery plan
  - Support the cleanup of the data center following an incident

Hardware Team

{The functionality provided below may also be relevant to these teams with appropriate modifications:

Hardware Salvage Team

Original Site Restoration/Salvage Coordination Team}

The Hardware team is responsible for site preparation, physical planning, and installation of data processing equipment to meet the required processing capability in the event of an incident. This includes responsibility for ordering and installing hardware and/or software necessary for both the alternate and permanent site.

- **Pre-disaster**:
  - Understand role and responsibilities within this plan
  - Work closely with the Contingency/Emergency Management Team to reduce possibilities for contingencies and disasters (See Preventive Measures in the Appendix)
  - Train employees in emergency preparedness
  - Participate in contingency exercises

- Know the procedures to be followed
- Maintain current system configuration information in an off-site storage facility and in this plan

- **Post-disaster:**
  - Verify with alternative site the pending occupancy requirements
  - Inspect the alternative site for physical space requirements
  - Interface with Software, Communications and Operations Team members on space configuration of alternative site
  - Coordinate transportation of salvageable equipment to the alternative site
  - Notify the Administration Team of equipment required
  - Ensure installation of required temporary terminals/PCs connected to the alternative site hardware
  - Plan the hardware installation at the alternative site
  - Plan, coordinate transportation of and installation of hardware at the permanent site, when available

Software Team

{The functionality provided below may also be relevant to the following teams with appropriate modifications:

Systems Software Team

Server Recovery Team (e.g., client server, Web Server)

LAN/WAN Recovery Team

Database Recovery Team

Application Recovery Team(s)

Telecommunications Team

Test Team

Network Operations Recovery Team

Operating Systems Administration Team}

The Software Team is responsible for the installation and configuration of all system and application software not installed by other administrators.

- **Pre-disaster**:
  - Understand role and responsibilities within this plan

- Work closely with the Contingency/Emergency Management Team to reduce possibilities for contingencies and disasters (See Preventive Measures in the Appendix)
- Train employees in emergency preparedness
- Participate in contingency exercises
- Know the procedures to be followed
- Maintain current system software configuration information in an off-site storage facility and in this plan

- **Post-disaster:**
  - Arrange for delivery of off-site storage containers containing backup media
  - Receive, inventory and control access to the off-site storage containers and media
  - Restore system/application software data files not installed in conjunction with another plan's personnel
  - Test and verify operating system/application software functionality as required
  - Return backup media storage containers to the off-site storage facility

Communications Team

The Communications Team is responsible for establishing voice and data links to/from the alternative site. This includes connecting local and remote users/customers to the alternate site.

- **Pre-disaster**:
  - Understand role and responsibilities within this plan
  - Work closely with the Contingency/Emergency Management Team to reduce possibilities for contingencies and disasters (See Preventive Measures in the Appendix)
  - Train employees in emergency preparedness
  - Participate in contingency exercises
  - Know the procedures to be followed
  - Maintain current communications configuration information in an off-site storage facility and in this plan

- **Post-disaster:**
  - Coordinate with the Damage Assessment Team on assessment of communications equipment
  - Retrieve communications configuration for the off-site storage facility
  - Plan, coordinate and install the necessary communications equipment at the alternate site

- Plan, coordinate and install the necessary cabling at the alternative sire not covered by other plan's recovery personnel

Physical/Personnel Security Team

Team is responsible for providing personnel identification and access limitations to the building and floors and acts as liaison with emergency personnel. This is crucial during the time of an incident because of the uncommonly large number of vendors, contractors and other visitors requiring access to the facility.

- **Pre-disaster**:
  - Understand role and responsibilities within this plan
  - Work closely with the Contingency/Emergency Management Team to ensure physical security of existing system and facilities
  - Train employees in emergency preparedness
  - Participate in contingency exercises
  - Know the procedures to be followed
- **Post-disaster:**
  - Cordon off the facility including offices to restrict unauthorized access
  - Coordinate with the Building Management for authorized personnel access
  - Provide additional physical security/guards
  - Act as liaison with emergency personnel, such as fire and police departments
  - Schedule and provide for security in transportation of files, reports, and equipment
  - Provide assistance to officials in investigating the damaged facility/site

Administration/Procurement Support Team

{This team comprises those functions of the following teams which might be separately specified if necessary:

- Transportation & Relocation Team
- Media Relations Team
- Legal Affairs Team}

The Administration Team is responsible for providing secretarial, filing, procurement, travel, housing, off-site storage, and other administrative matters not performed by other team members. Included is limited authority to provide funds for emergency expenditures other than for capital equipment and salaries. This Team is also responsible for effecting all dissemination of

information to the Department's Media Relations Officer, and working with the Department's Legal Representation staff on all related matters.

- **Pre-disaster**:
    - Understand role and responsibilities within this plan
    - Work closely with the Contingency/Emergency Management Team to ensure all administrative functions are accomplishable
    - Work closely with the Contingency/Emergency Management Team to ensure all potential means of transportation are understood and provided for
    - Train employees in emergency preparedness
    - Participate in contingency exercises
    - Know the procedures to be followed
    - Ensure details of administering emergency funds expenditures are known
    - Assess need for alternative means of communication (other than normal telephone service) is available to all employees involved
    - Maintain current listings of prospective means and modes of transportation to the alternate site are viable and included at the off-site storage location and in the appendix to this plan
    - Maintain contact information for the Department's Media Relations Officer, and the Department's Legal Representation staff. Information is stored at the off-site storage facility and is included in the appendix to this plan.
- **Post-disaster:**
    - Prepare, coordinate, and obtain approval for all procurement requests
    - Coordinate deliveries
    - Process requests for payment of all invoices related to the incident
    - Arrange for travel and lodging of members involved in the incident
    - Provide for acquisition of telephone equipment and capabilities/services including voice, dial-up, and leased lines
    - Provide for alternative means of communications among the teams in the event that normal telephone services are unavailable
    - Arrange for temporary secretarial support for filing, and other administrative services required by the various teams
    - Coordinate with other teams to provide any specific transportation needs
    - Plan, coordinate and provide transportation to the alternate site, as necessary
    - Perform all tasks with the Department's Media Relations Officer, and working with the Department's Legal Representation staff on all related matters as directed by the Contingency/Emergency Management Team

5 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 Chief Information Officer or IT Contingency Planning Coordinator.

> **In an emergency, the *CBP* 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 B of this plan. The notification sequence is listed below:

- The first responder is to notify the System Owner / IT Contingency Planning Coordinator. All known information must be relayed to the System Owner / IT Contingency Planning Coordinator.
- The systems manager is to contact the Damage Assessment Team (DAT) Leader and inform them of the event. The System Owner / IT Contingency Planning Coordinator is to instruct the DAT Leader to begin assessment procedures.
- The DAT 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 DAT 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 {*System Owner / IT Contingency Planning Coordinator}*, the Damage Assessment Team Leader is to …
- *{The Damage Assessment Team}* is to ….

Alternate Assessment Procedures:

- Upon notification from the {*System Owner / IT 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 {*System Owner / IT Contingency Planning Coordinator}* of the results.

  − The {*System Owner / IT 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 {*System Owner / IT Contingency Planning Coordinator}* is to notify civil emergency personnel (e.g., police, fire) assessment of the results, as appropriate.

The IT Contingency Plan is to be activated if one or more of the following criteria are met:

1. {*System name}* will be unavailable for more than {48} hours.
2. Facility is damaged and will be unavailable for more than {24} hours
3. Other criteria, as appropriate.

If the plan is to be activated, the {*System Owner / IT 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 {*System Owner / IT Contingency Planning Coordinator}*, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepare to respond and relocate if necessary.

The {*System Owner / IT 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 {*System Owner / IT 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 {*System Owner / IT Contingency Planning Coordinator}* is to notify remaining personnel (via notification procedures) on the general status of the incident.

6 RECOVERY PHASE

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 within the allowable outage time of *{number of hours/days}* as determined by the Business Impact Analysis (BIA).

Recovery Goal. {*State the first recovery objective as determined by the BIA if available. 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}.

7 RECONSTITUTION (RETURN TO NORMAL OPERATIONS) PHASE

This section discusses activities necessary for restoring {*system name*} operations at the CBP 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.

7.1 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}*

7.2 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}*

7.3 Plan Deactivation

{Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the CBP, 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}*

8 PLAN APPENDICES

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

8.1 Personnel Contact Procedure and Team Contact Listings:

{Note that a special "Residual/Other" Team Contact List should be prepared for individuals not already included in other teams. This special contact list will be used to keep the uninvolved personnel aware of status and activities that may require action on their part}.

Notification Procedure

The team leader, alternate or assigned individual upon activation of the Business Resumption Plan will contact team personnel using the following procedure:

During notifications of an alert or declared disaster, use this procedure to alert all personnel. Read the procedures thoroughly prior to making a call**. By using the following instructions, you will not unnecessarily alarm family members of an employee who was working at the affected site at the time of the disaster.**

Place phone call and say, "May I speak with (individual name)?"

1. If available, provide the information you called to convey.
   - Remind the person to make no public statements about the situation.
   - Remind the person not to call co-workers (unless instructed to) and to advise their family not to call other employees.
   - Record the information in the contact status column.

2. If not available, say, "Where may I reach (individual)?"
   - If at any location other than the data center, get the phone number. Call the other location and providing the information you wanted to convey.
   - **If the individual was working at the affected site, indicate that you will reach the individual there. DO NOT discuss the disaster with the person answering the phone.**
   - **Immediately notify the Emergency Operations Center.**
   - Record the information in the contact status column.

3. If contact is made with an answering machine: Make no statement regarding the situation. Provide the phone number to call at Emergency Operations Center; ask that the employee make contact at that number as soon as possible.
   - Record the information in the contact status column.

4. If no answer:
   - Record the information in the contact status column.

5. If no answer and the individuals have an alternate voice communication capability:

- Place a call to the beeper number.
- Enter the number of the Emergency Operations Center for the individual to call.
- Record the information in the contact status column.

Notification Information:

Using the team member contact list, see following pages, the team leader, alternate or assigned individual should convey the following information when contacting the team personnel:

- **Brief description of the problem.**
- **Location of the Emergency Operations Center and / or the Business Recovery Site**
- **Phone number of the Emergency Operations Center.**
- **Immediate actions to be taken.**
- **Whether or not the facility can be entered.**
- **Location and time the team should meet.**
- **All team members should carry photo identification with them at all times and be prepared to show it to security or local authorities.**
- **Instruct everyone notified not to make any statements to the media.**

All callers should record status of everyone they call, noting the time the call was placed and whether the person was contacted. Make a reasonable number of attempts if the phone was busy or there was no answer. Forward the completed list to the EOC and the staff will continue to attempt to contact team members.

{Indent names to indicate the organization of the calling tree (who calls who). Calling trees for a large group of personnel should be designed to limit the number of individuals that are called by a single individual to no more than 3 or 4. This will provide for expeditious communications with all team members. It will also minimize and provide for those situations where an individual must contact subordinates to those individuals that cannot be directly contacted}.

Team: {Contingency Management Team}

Name (Team Position)	Phone Numbers (Home, Cell, Office)	Contacted (Date & Time)	Comments
John Doe Team Leader	301-555-1234 (H) 703-555-2345 (C) 202-555-3456 (O)		
Mary Smith (Team Lead Alternate)	301-555-1234 (H) 703-555-2345 (C) 202-555-3456 (O)		
Bob Jones (Member)	301-555-1234 (H) 703-555-2345 (C) 202-555-3456 (O)		
Sam Smith (Member)	301-555-1234 (H) 703-555-2345 (C) 202-555-3456 (O)		

8.2 Personnel Roster – Full Detail – Alphabetical Order

{This is a detailed roster containing all information derived & produced from information collected via the recommended template in Appendix A}

Adams, John

Contact Info. Phone Home: 301-555-1234 Phone Cell: 703-555-2345
Phone Office: 202-555-3456
Pager: 410-555-4567 Blackberry 240-555-5678
Personal Email: jadams@xyz.net

Home Address: 123 First Street
Hometown, DC 20001
Office Address: GSA Bldg.
4025-01
300 7th Street SW
Washington, DC 20001
Emergency Contact: Adams, Mary
123 First Street
Hometown, DC 20001
Phone Home: 301-555-4321 Phone Cell: 703-555-5432
COOP Team Relocation: Yes
Special Capabilities: Windows Server Admin, Spanish, Certified First Aid, Certified CPR, 4 WD Truck

Doe, John

Contact Info. Phone Home: 301-555-1234 Phone Cell: 703-555-2345
Phone Office: 202-555-3456
Pager: 410-555-4567 Blackberry 240-555-5678
Personal Email: jdoe@abc.com
Home Address: 1001 First Street
Hometown, MD 20701
Office Address: GSA Bldg.
4025-01
300 7th Street SW
Washington, DC 20001
Emergency Contact: Doe, Mary
1001 First Street
Hometown, DC 20701

Phone Home: 301-555-4321 Phone Cell: 703-555-5432

COOP Team Relocation: Yes

Special Capabilities: MS- Office, French, Portable Boat, Camper

8.3 Vendor Contacts:

(When needed -include multiple contacts for a single vendor in separate rows)

Vendor Product/Service	Contact Name / Address	Phone Numbers (Home, Cell, Office, FAX, 24 hour)	Contacted (Date & Time)	Comments
Equipment Inc. Misc. Equipment	John Doe Sales & Marketing 123 Main Street Midtown, MA 12345	301-555-1234 (H) 703-555-2345 (C) 202-555-3456 (O) 202-555-7890 (F) 301-555-6789 (24h)		

8.4 Emergency Operations Control Log

{Log will be utilized at all locations and by all teams during contingency recovery activities}

Date: **Recorder:**

Time	Caller Name & Phone #	Person Called	Reason:	Status or Comments

8.5 Customer Contacts:

(When needed - include multiple contacts for a single customer in separate rows)

Customer Product/Service	Contact Name / Address	Phone Numbers (Home, Cell, Office, FAX, 24 hour)	Contacted (Date & Time)	Comments
Dept XYZ Primary User	**John Doe Sales & Marketing 123 Main Street Midtown, MA 12345**	**301-555-1234 (H) 703-555-2345 (C) 202-555-3456 (O) 202-555-7890 (F) 301-555-6789 (24h)**		

8.6 Preventive Controls:

Appropriate personnel associated with the {system} are trained on how and when to use these controls. These controls are maintained in good condition to ensure their effectiveness in an emergency.

Following are those utilized controls.

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls)
- Gasoline- or diesel-powered generators to provide long-term backup power
- Air-conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor
- Fire suppression systems
- Fire and smoke detectors
- Water sensors in the computer room ceiling and floor
- Plastic tarps that may be unrolled over IT equipment to protect it from water damage
- Heat-resistant and waterproof containers for backup media and vital nonelectronic records
- Emergency master system shutdown switch
- Offsite storage of backup media, non-electronic records, and system documentation
- Technical security controls, such as cryptographic key management and least-privilege access controls
- Frequent, scheduled backups.

8.7 Equipment and Specifications

Manufacturer	Model	Specifications (Include all necessary information to adequately define the item)	Quantity	Comments

8.8 Vital Records (electronic and hard copy)

{Include information on all vital records that are needed for contingency recovery and resumption activities and those that may be needed for continued operation}.

Record	Description	Owner	User	Classification	Storage Location	Need Access At

8.9 Service Level Agreements and Memorandums of Understanding

{Include all relevant documentation}

8.10 Backup Operations Plan

{Include all documentation that is related to backup and restoration of this system/application for an immediate or even extended period of time}

8.11 Written Access Controls Policies and Procedures

{Include all documentation that is related access controls policies and procedures of this system/application}

8.12 Standard Operating Procedures

{Include all documentation that is related to recovery, resumption, and operation of this system/application for an immediate or even extended period of time}

8.13 Related IT Contingency Plans

{Include all related IT Contingency Plans for overarching and/or subordinate systems/applications}

8.14 Emergency Management Plan

{Include copies of other related Emergency Management Plans}

8.15 Occupant Evacuation Plan

{Include copies of the plans for the primary and alternate sites}

8.16 Continuity of Operations Plan

{Include copies of any Continuity of Operations Plans (COOP)}

8.17 Team Task Checklists

{Team Task Checklists should be included using the following recommended format or other suitable format. There should be a checklist for each team assigned or utilized in this IT Contingency Plan. Include at strategic intervals communications with the Emergency Control Center and/or Emergency Management Team.}

Team Name: _____

Task Id #	Activity	Comments	Date & Time Completed
1	Advise ECC/EMT of arrival.		

8.18 Primary & Alternate Site Locations, and Travel Directions/Maps

Primary Location	
Facility Name:	
Street Address:	**Floor:**
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No:** **24 Hour No:** **FAX No:** **Other No.:**
Security Considerations:	

Alternate Location	
Facility Name:	
Street Address:	**Floor:**
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No:** **24 Hour No:** **FAX No:** **Other No.:**
Security Considerations:	

Directions to Alternate Recovery Site(s):

{Directions should be provided from the primary to the alternate site, and also from local landmark locations where possible}

8.19 Alternate Site/Locations Hotel and Restaurant Information

{Include hotel names, addresses, and phone numbers and local restaurant information}

8.20 Orders of Succession and Delegations of Authority

{Include copies of all signed Orders of Succession and Delegations of Authority that are relevant to this plan and the organizations. Include those for Senior Level Management.}

8.21 Emergency Contact Quick Reference Information

{Include the phone numbers for the Emergency Recovery Control Center, Relocation Team Offices, and Telephone Answering Machines for Status Update Recordings, etc.}

Name/Title	Phone Number	Comments
Contingency Management Team	**301-555-1234**	Call with status updates minimally at every two hour intervals or as otherwise advised**.**
Site A Relocation Team	**703-555-2345**	
DHS Information Line	**999-555-5432**	This is an answering machine with a periodically updated recording of information relative to recovery and relocation. Call minimally at four hour intervals to remain current of overall DHS status. **DO NOT PROVIDE THIS NUMBER TO ANYONE INCLUDING THE PUBLIC MEDIA.**

8.22 System/Application Recovery Priority Classification

{Include a copy of signed documentation that prioritizes the recovery of Systems and/or Applications that are overarching or subordinate to the recovery of {system name}.

System Name	Priority	Original Site/Location	Recovery Site/Location

8.23 Off-Site Storage

{Include information for all off-site storage locations}

Company/Facility Name:	
Street Address:	**Floor:**
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No:** **24 Hour No:** **FAX No:** **Other No.:**
Considerations:	

{Include the names etc. of those individuals that may recall media and/or documents from the off-site storage location}

Name	Phone Numbers (Home, Cell, Office)	Contacted (Date & Time)	Comments
John Doe	**301-555-1234 (H)** **703-555-2345 (C)** **202-555-3456 (O)**		**Chief Librarian & COTR**
Mary Smith	**301-555-1234 (H)** **703-555-2345 (C)** **202-555-3456 (O)**		
Bob Jones	**301-555-1234 (H)** **703-555-2345 (C)** **202-555-3456 (O)**		
Sam Smith	**301-555-1234 (H)** **703-555-2345 (C)** **202-555-3456 (O)**		

{Include directions to off-site Storage as necessary}

Directions:

8.24 Business Impact Analysis

{Attach a copy of the complete BIA}

8.25 Personnel Information Collection Document

Employee Information:

Employee ID

Name

Title

Street Address

Address 2

Address 3

City State Zip & Ext

Personal Email

Contact Phone Nos.:

Home

Work

Pager Pin # Pager

Cell Cell Ext/ Nextel DC Code

Alt Type Alternate

Work Information:

Contractor (y/n) Company if Yes _____

Work Schedule

Off Day

Work Shift

Email

Level 1 Employee (y/n)

COOP Relocation Employee (y/n)

Relocation Site Trans Mode

Emergency Contact Information:

Name

Phone #'s

Work

Home

Alternate Type Alternate

Address:

Street

City State Zip & Ext

Attributes (circle all that apply):

Personally Owned Equipment:

Has a personally owned cell phone

Has a personally owned desktop computer

Has a personally owned notebook computer

Certified Skill:

Notary Public

Certified Scuba Diver

Volunteer Firefighter

Communications Resources:

Owns a CB radio

Owns a Family Radio Service (FRS) radio

Owns a shortwave radio (receive capability)

Licensed shortwave radio operator

Computing Resources:

Data Communication Network Skills

PC Desktop Support

Admin Microsoft Windows Administration

Support PC LAN Support

Network/Data Communication Specialists

Network/Data Communications

Resources/Services:

Voice Communication Network Skills

HW Computer Hardware Expertise

Computer Operations Support Specialists

HW Computer System Hardware Specialists

Computer Programming Support Specialists

Computer Programming Support

Computer System Software Specialists

Applications Programmer/Analyst

Seagate Crystal Reports trained

Data Entry Specialists

Microsoft Office

Microsoft Access Trained

Microsoft Excel Trained

Microsoft Internet Information Server (IIS) Trained

Microsoft PowerPoint Trained

Microsoft Project Trained

Microsoft SQL Trained

Microsoft Windows Trained

Microsoft Windows Admin Trained

Microsoft Word Trained

Novell Netware Trained

Oracle Trained

BIA Professional Trained

BCP/DR Trained

Incident Manager Trained

Sybase Trained

Telecommunication Expertise

Web Application Specialist

DTS Web Support

Government Issued:

Participates in Alternate Work Schedule Program

Government issued cell phone

Government credit purchase card with $2,500 spending limit per transaction

Government credit purchase card with $200K spending limit per transaction

Government issued desktop PC for home use

Approved Request for dial-in access

Authorized Work at Home Program

Work From Home Back-Up Capability:

Government issued notebook computer

Government phone line installed at home

Government Secure Identification Card

Government Calling Card

Government Travel Credit Card

Language Skills:

Proficient in Sign Language

Speaks Arabic

Speaks Chinese

Speaks French

Speaks German

Speaks Hebrew

Speaks Italian

Speaks Japanese

Speaks Korean

Speaks Norwegian

Speaks Polish

Speaks Portuguese

Speaks Russian

Speaks Spanish

Speaks Swedish

Medical Training

Trained in the use of an Automated External Defibrillator

CPR Certified

Medical Doctor

Emergency Medical Technician

Registered Nurse

Office Skills/Administration

Lives within 4 miles work center

Telephone Answering Services

Knowledge of Business Continuity Policies

Budget planning/involvement

Business Unit/Process Personnel

Business Unit/Process Specialists

Business Unit/Process Resources/Services

Centralized Telephones

Acquisition Management

Contracting Officer--Unlimited Warrant

Contracting Officers Technical Representative

Purchases furniture, equipment, supplies

Copying/Faxing Services

Personal Counseling Services

Customer Representative

IT Security Specialist - Incident Response

Executive Mgt Director and above

Facilities Support Specialists

Facilities Support Resources/Services

Authorized to Sign Property Removal Permit

Authorized to Sign Property Loan Permit

Health and Safety Officer

Knowledge of IRM policies and standards

IT Security Specialist

Mail Distribution/Delivery/Copying Assistance

Scheduling Meetings/Conference Rm/Database Assistance

Personnel actions, recruits, reassignments, etc.

Procurement Desktop Trained

Processing/Fulfillment Services

Professional Services

Coordinator of Reading Files

Records management expertise

Recovery Support Resources/Services

Recovery Support Specialists

Risk Management Specialist

Student Registration

Knowledge of Surety Bond Process & Procedures

Time-Keeper Function

Travel Assistance

Trade Skills

Cubical Setup Skills

Electrical Skills

Plumbing Skills

Roofing Skills

Transportation Resources

Not a licensed driver

Owns a 4 wheel drive vehicle

Has a Commercial Drivers License

Owns a motor boat

Owns a pick-up truck

Licensed Pilot

Owns a 2 or more passenger airplane

Owns a vehicle with a snow plow

Owns a motor home recreational vehicle

Owns a cargo trailer

Owns a small un-powered boat or canoe