<Project Name>

<System Name>

Information Technology Contingency Plan

Version Number: 1.0

Version Date: <mm/dd/yyyy>

VERSION HISTORY

[Provide information on how the development and distribution of the Security Approach will be controlled and tracked. Use the table below to provide the version number, the author implementing the version, the date of the version, the name of the person approving the version, the date that particular version was approved, and a brief description of the reason for creating the revised version.]

Version Number	Implemented By	Revision Date	Approved By	Approval Date	Description of Change
1.0	*<Author name>*	*<mm/dd/yy>*	*<name>*	*<mm/dd/yy>*	*<description of change>*

Notes to the Author

[This document is a template of a Security Approach document for a project. The template includes instructions to the author, boilerplate text, and fields that should be replaced with the values specific to the project.

- *Blue italicized text enclosed in square brackets ([text]) provides instructions to the document author, or describes the intent, assumptions and context for content included in this document.*
- *Blue italicized text enclosed in angle brackets (<text>) indicates a field that should be replaced with information specific to a particular project.*
- *Text and tables in black are provided as boilerplate examples of wording and formats that may be used or modified as appropriate to a specific project. These are offered only as suggestions to assist in developing project documents; they are not mandatory formats.*

When using this template, the following steps are recommended:

1. *Replace all text enclosed in angle brackets (e.g., <Project Name>) with the correct field document values. These angle brackets appear in both the body of the document and in headers and footers. To customize fields in Microsoft Word (which display a gray background when selected) select File->Properties->Summary and fill in the appropriate fields within the Summary and Custom tabs.*

   After clicking OK to close the dialog box, update all fields throughout the document selecting Edit>Select All (or Ctrl-A) and pressing F9. Or you can update each field individually by clicking on it and pressing F9.

   These actions must be done separately for any fields contained with the document's Header and Footer.
2. *Modify boilerplate text as appropriate for the specific project.*
3. *To add any new sections to the document, ensure that the appropriate header and body text styles are maintained. Styles used for the Section Headings are Heading 1, Heading 2 and Heading 3. Style used for boilerplate text is Body Text.*
4. *To update the Table of Contents, right-click on it and select "Update field" and choose the option - "Update entire table".*
5. *Before submission of the first draft of this document, delete this instruction section "Notes to the Author" and all instructions to the author throughout the entire document.]*

Table of Contents

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 BACKGROUND

This *<System Name>* Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a) (7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

This *<System Name>* Contingency Plan is promulgated under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems" dated June 2002.

1.3 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*>*.*

1.4 SCOPE

1.4.1 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.

1.4.2 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.

1.5 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 48 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. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below. *[Continue description of succession as applicable.]*

Contact List

#	Name	Office Phone	Home Phone	Cell Phone	Email
1	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>
2	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>
3	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>
4	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>
5	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>	<Click here and enter data>
14	<Click here and	<Click here	<Click here	<Click here and	<Click here

#	Name	Office Phone	Home Phone	Cell Phone	Email
	enter data>	and enter data>	and enter data>	enter data>	and enter data>

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]

2.4 TESTING AND MAINTENANCE

The Business Owner and System Developer/Maintainer shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the table top testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

2.4.1 Tabletop Testing

Tabletop Testing should be conducted in accordance with the CMS Contingency Planning Tabletop Test Procedures. The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis; and

- Crisis communications and call tree verification.

2.4.2 Technical Testing

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch voice and data telecommunications to alternate processing site.

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>* and inform them of the event. The *<Contingency Planning Coordinator>* is to instruct the Team Leader to begin assessment procedures.
- The *<Damage Assessment Team>* 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
- *<Damage Assessment Team Leader>* 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 Contingency Plan. 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 CP. 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 CP). 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.

5.1 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*

5.2 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*

5.3 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*

Appendix A: Contingency Plan Approval

The undersigned acknowledge that they have reviewed the ***<System Name>*** **Contingency Plan** and agree with the information presented within this document. Changes to this **Contingency Plan** will be coordinated with, and approved by, the undersigned, or their designated representatives.

[List the individuals whose signatures are desired. Examples of such individuals are Business Owner, Project Manager (if identified), Designated Approving Authorities and any appropriate stakeholders. Add additional lines for signature as necessary.]

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

APPENDIX B: REFERENCES

[Insert the name, version number, description, and physical location of any documents referenced in this document. Add rows to the table as necessary.]

The following table summarizes the documents referenced in this document.

Document Name	Description	Location
<Document Name and Version Number>	*<Document description>*	*<URL or Network path where document is located>*

APPENDIX C: KEY TERMS

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Term	Definition
[Insert Term]	*<Provide definition of term and acronyms used in this document.>*

APPENDIX D: RELATED DOCUMENTS

- **FIPS 199**, *Standards for Security Categorization of Federal Information and Information Systems*
- **FIPS 200**, *Minimum Security Requirements for Federal Information and Information Systems*
- **SP 800-18**, *Guide for Developing Security Plans for Federal Information Systems*
- **SP 800-30**, *Risk Management Guide for Information Technology Systems*
- **SP 800-37**, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- **SP 800-53**, *Recommended Security Controls for Federal Information Systems*
- **Draft SP 800-53A**, *Guide for Assessing the Security Controls in Federal Information Systems*
- **SP 800-55**, *Security Metrics Guide for Information Technology Systems*
- **SP 800-60**, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- **SP 800-70**, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*
- **SP 800-100**, *Information Security Handbook: A Guide for Managers*