Information System Contingency Plan Template

<Vendor>

<Information System Name>
Version x.x

Month dd, 20yy

Company Sensitive and Proprietary
For Authorized Use Only

Information Technology Contingency Plan

Prepared by

Identification of Organization that Prepared this Document		
<insert logo>	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Prepared for

Identification of Cloud Service Provider		
<insert logo>	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Template Revision History

Date	Page(s)	Description	Author
06/06/2014		Major revision for SP800-53 Revision 4. Includes new template and formatting changes.	FedRAMP PMO

Table of Contents

Executive Summary ..... **Error! Bookmark not defined.**
Template Revision History 3
About this document 7
Who should use this document? 7
How this document is organized 7
How to contact us 8
Contingency Plan Approvals 9
1. Introduction and Purpose 10
1.1. Applicable Laws and Regulations ..... **Error! Bookmark not defined.**
1.2. Applicable Standards and Guidance ..... **Error! Bookmark not defined.**
1.3. Information System Name and Identifier 12
1.4. Scope 12
1.5. Assumptions 12
2. Concept of Operations 13
2.1. System Description 13
2.2. Three Phases 13
2.3. Data Backup Readiness Information 14
2.4. Site Readiness Information 15
2.5. Roles and Responsibilities 16
2.5.1. Contingency Planning Director (CPD) 16
2.5.2. Contingency Planning Coordinator 17
2.5.3. Outage and Damage Assessment Lead (ODAL) 17
2.5.4. Hardware Recovery Team 17
2.5.5. Software Recovery Team 18
2.5.6. Telecommunications Team 18
2.5.7. Procurement and Logistics Coordinator (PLC) 18
2.5.8. Security Coordinator 19
2.5.9. Plan Distribution and Availability 19
2.5.10. Line of Succession/Alternates Roles 20
3. Activation and Notification 20
3.1. Activation Criteria and Procedure 20
3.2. Notification Instructions 20

3.3. Outage Assessment 21
4. Recovery 21
4.1. Sequence of Recovery Operations 21
4.2. Recovery Procedures 21
4.3. Recovery Escalation Notices/Awareness 22
5. Reconstitution 22
5.1. Data Validation Testing 22
5.2. Functional Validation Testing 22
5.3. Recovery Declaration 22
5.4. User Notification 23
5.5. Cleanup 23
5.6. Returning Backup Media 23
5.7. Backing up Restored Systems 23
5.8. Event Documentation 24
6. Contingency Plan Testing 24
Appendix A – Key Personnel and Team Member Contact List 25
Appendix B – Vendor Contact List 26
Appendix C.1 – Alternate Storage Site Information 27
Appendix C.2 – Alternate Processing Site Information 28
Appendix C.3 – Alternate Telecommunications Provisions 29
Appendix D – Alternate Processing Procedures 30
Appendix E – System Validation Test Plan 31
Appendix F – Contingency Plan Test Report 32
Appendix G – Diagrams 33
Appendix H – Hardware and Software Inventory 34
Appendix I – System Interconnections 35
Appendix J – Test and Maintenance Schedule 36
Appendix K – Associated Plans and Procedures 37
Appendix L – Business Impact Analysis 38

List of Tables

Table 1-1 Information System Name and Title 12
Table 2-1 Backup Types 14
Table 2-2 Backup System Components 15
Table 2-3 Alternative Site Types 16
Table 2-4 Primary and Alternative Site Locations 16
Table 3-1 Personnel Authorized to Activate the ISCP 20
Table 5-1 Cleanup Roles and Responsibilities 23
Table 5-2 Event Documentation Responsibility 24

ABOUT THIS DOCUMENT

This document contains the template that CSPs are required to use when submitting an Information System Contingency plan to the FedRAMP PMO as part of a FedRAMP assessment.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by Cloud Service Providers (CSPs), Independent Assessors (3PAOs), government contractors working on FedRAMP projects, government employees working on FedRAMP projects, and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into six primary sections and fourteen appendices.

Section 1	Describes the introduction section which orients the reader to the type and location of information contained in the plan.
Section 2	Describes concept of operations and provides additional details about the information system, the three phases of the contingency plan (Activation and Notification, Recovery, and Reconstitution), and a description of the information system contingency plan roles and responsibilities.
Section 3	Describes the Activation and Notification Phase and defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan.
Section 4	Describes the Recovery Phase activities and focuses on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location.
Section 5	Describes the Reconstitution Phase which is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality.
Section 6	Describes how the ISCP must be tested.
Appendix A	Key Personnel and Team Member Contact List
Appendix B	Vendor Contact List
Appendix C.1	Alternate Storage Site Information
Appendix C.2	Alternate Processing Site Information
Appendix	Alternate Telecommunications Site Information

C.3	
Appendix D	Alternate Processing Procedures
Appendix E	System Validation Test Plan
Appendix F	Contingency Plan Test Report
Appendix G	Diagrams
Appendix H	Hardware and Software Inventory
Appendix I	System Interconnections
Appendix J	Test and Maintenance Schedule
Appendix K	Associated Plans and Procedures
Appendix L	Business Impact Analysis

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to *info@fedramp.gov*.

For more information about FedRAMP, see http://www.fedramp.gov.

CONTINGENCY PLAN APPROVALS

x
<Name> **<Date>** **<Title>** **<Cloud Service Provider>**
x
<Name> **<Date>** **<Title>** **<Cloud Service Provider>**
x
<Name> **<Date>** **<Title>** **<Cloud Service Provider>**
x
<Name> **<Date>** Authorizing Official

1. INTRODUCTION AND PURPOSE

Information systems are vital to **<Cloud Service Provider>** mission/business functions; therefore, it is critical that services provided by **<Information System Name>** are able to operate effectively without excessive interruption. This Information Technology Contingency Plan (ISCP) establishes comprehensive procedures to recover **<Information System Name>** quickly and effectively following a service disruption.

One of the goals of an IT Contingency Plan is to establish procedures and mechanisms that obviate the need to resort to performing IT functions using manual methods. If manual methods are the only alternative; however, every effort must be made to continue IT functions and processes manually.

The nature of unprecedented disruptions can create confusion, and often predisposes an otherwise competent IT staff towards less efficient practices. In order to maintain a normal level of efficiency, it is important to decrease real-time process engineering by documenting notification and activation guidelines and procedures, recovery guidelines and procedures, and reconstitution guidelines and procedures prior to the occurrence of a disruption. During the notification/activation phase, appropriate personnel are apprised of current conditions and damage assessment begins. During the recovery phase, appropriate personnel take a course of action to recover the **<Information System Name>** components a site other than the one that experienced the disruption. In the final, reconstitution phase, actions are taken to restore IT system processing capabilities to normal operations.

1.1. APPLICABLE LAWS AND REGULATIONS

- Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

1.2. APPLICABLE STANDARDS AND GUIDANCE

- A NIST Definition of Cloud Computing [NIST SP 800-145]
- Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
- Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
- Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Guide to Understanding FedRAMP Version 1.2, April 22, 2013 Page 12 Revision 1]
- Guide for Developing the Risk Management Framework to Federal Information Systems:
- A Security Life Cycle Approach [NIST SP 800-37, Revision 1] Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1]
- Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Managing Information Security Risk [NIST SP 800-39]
- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
- Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 3]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

1.3. FEDRAMP REQUIREMENTS AND GUIDANCE

All FedRAMP documents are available at www.fedramp.gov

- FedRAMP Incident Communications Procedure
- FedRAMP Continuous Monitoring Strategy and Guide
- Guide to Understanding FedRAMP

1.4. INFORMATION SYSTEM NAME AND IDENTIFIER

This ISCP applies to the **<Information System Name>** which has a unique identifier as noted in Table 1-1.

Unique Identifier	Information System Name	Information System Abbreviation

Table 1-1 Information System Name and Title

1.5. SCOPE

This ISCP has been developed for **<Information System Name>** which is classified as a **<Moderate/Low>** impact system, in accordance with Federal Information Processing Standards (FIPS) 199. FIPS 199 provides guidelines on determining potential impact to organizational operations and assets, and individuals through a formula that examines three security objectives: confidentiality, integrity, and availability. The procedures in this ISCP have been developed for a **<Moderate/Low>** impact system and are designed to recover the **<Information System Name>** within **<Recovery Time Objective (RTO) hours>**. The replacement or purchase of new equipment, short-term disruptions lasting less than **<RTO hours>**, or loss of data at the primary facility or at the user-desktop levels is outside the scope of this plan.

Instruction: Edit the below list to name other plans and circumstances that are related but are outside the scope of this ISCP.

This ISCP does not apply to the following situations:

- **Overall recovery and continuity of mission/business operations.** The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of business operations.
- **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) addresses employee evacuation.

1.6. ASSUMPTIONS

Instruction: A list of default assumptions are listed in the section that follows. The assumptions must be edited, revised, and added to so that they accurately characterize the information system described in this plan.

The following assumptions have been made about the <Information System Name>:

- The Uninterruptable Power Supply (UPS) will keep the system up and running for <total number of seconds/minutes>
- The generators will kick in after <total number of seconds/minutes> from time of a power failure

- Current backups of the application software and data are intact and available at the offsite storage facility in <City, State>
- The backup storage capability is approved and has been accepted by the AO
- The **<Information System Name>** is inoperable if it cannot be recovered within **<RTO hours>**
- Key personnel have been identified and are trained annually in their roles
- Key personnel are available to activate the ISCP
- **<Cloud Service Provider>** defines circumstances that can inhibit recovery and reconstitution to a known state

2. CONCEPT OF OPERATIONS

This section provides details about the **<Information System Name>**, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of the roles and responsibilities of key personnel during contingency operations.

2.1. SYSTEM DESCRIPTION

Instruction: Provide a general description of the system architecture and components. Include a network diagram that indicates interconnections with other systems. Ensure that this section is consistent with information found in the System Security Plan. Provide a network diagram and any other diagrams in Appendix G.

2.2. THREE PHASES

This plan has been developed to recover and reconstitute the **<Information System Name>** using a three-phased approach. The approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. The three system recovery phases consist of activation and notification, recovery, and reconstitution.

1. **Activation and Notification Phase.** Activation of the ISCP occurs after a disruption, outage, or disaster that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

   Once the ISCP is activated, the information system stakeholders are notified of a possible long-term outage, and a thorough outage assessment is performed for the information system. Information from the outage assessment is analyzed and may be used to modify recovery procedures specific to the cause of the outage.

2. **Recovery Phase.** The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level such that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and

awareness escalation procedures for communication of recovery status to system stakeholders.

3. **Reconstitution.** The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating data and operational functionality followed by deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

2.3. DATA BACKUP READINESS INFORMATION

A common understanding of data backup definitions is necessary in order to ensure that data restoration is successful. **<Cloud Service Provider>** recognizes different types of backups which have different purposes and those definitions are found in Table 2-1.

Backup Type	Description
Full Backup	A full backup is the starting point for all other types of backup and contains all the data in the folders and files that are selected to be backed up. Because full backup stores all files and folders, frequent full backups result in faster and simpler restore operations
Differential Backup	Differential backup contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if the differential backup is performed too many times, the size of the differential backup might grow to be larger than the baseline full backup.
Incremental Backup	Incremental backup stores all files that have changed since the last FULL, DIFFERENTIAL OR INCREMENTAL backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup must be processed, which may result in a lengthy restore job.
Mirror Backup	Mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the source data.

Table 2-1 Backup Types

The hardware and software components used to create the **<Information System Name>** backups are noted in Table 2-2.

System/Component	Description
Software Used	
Hardware Used	
Frequency	
Backup Type	
Retention Period	

Table 2-2 Backup System Components

Current backups of the **<Information System Name>** system software and data are intact and available at the offsite storage facility located at:

<Site Name>

<Street Address>

<City, State, Zip Code>

Personnel who are authorized to retrieve backups from the offsite storage location, and may authorize the delivery of backups, are noted in Appendix C.1.

<Cloud Service Provider> maintains both an online and offline (portable) set of backup copies of the following types of data on site at their primary location:

user-level information
system-level information
information system documentation including security information.

2.4. SITE READINESS INFORMATION

<Cloud Service Provider> recognizes different types of alternate sites, which are defined in Table 2-3.

Type of Site	Description
Cold Sites	Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
Warm Sites	Warm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.
Hot Sites	Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.
Mirrored Sites	Mirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

Table 2-3 Alternative Site Types

Alternate facilities have been established for the **<Information System Name>** as noted in Table 2-4. Detailed information about the alternate processing site, the alternate storage site, and alternate telecommunications can be found in Appendix F.

Designation	Site Name	Site Type	Address
Primary Site			
Alternate Site			
Alternate Site			

Table 2-4 Primary and Alternative Site Locations

2.5. ROLES AND RESPONSIBILITIES

<Cloud Service Provider> establishes multiple roles and responsibilities for responding to outages, disruptions, and disasters for the **<Information System Name>**. Individuals who are assigned roles for recovery operations collectively make up the Contingency Plan Team and are trained annually in their duties. Contingency Plan Team members are chosen based on their skills and knowledge.

Instruction: Describe each team and role responsible for executing or supporting system recovery and reconstitution. Include responsibilities for each team/role including leadership roles. FedRAMP has established default roles and a small set of default responsibilities which must be edited and modified to match the actual organizational role names, responsibilities, and associated duties for the organization.

The Contingency Plan Team consists of personnel who have been selected to perform the roles and responsibilities described in the sections that follow. All team leads are considered key personnel.

2.5.1. CONTINGENCY PLANNING DIRECTOR (CPD)

The Contingency Planning Director (CPD) is a member of senior management and owns the responsibility for all facets of contingency and disaster recovery planning and execution.

The CPD performs the following duties:

- Makes the decision on whether or not to activate the ISCP
- Provides the initial notification to activate the ISCP
- Reviews and approves the ISCP
- Reviews and approves the Business Impact Analysis (BIA)
- Notifies the Contingency Plan Team leads and members as necessary
- Advises other Contingency Plan Team leads and members as appropriate
- Issues a recovery declaration statement after the system has returned to normal operations

- Designates key personnel

2.5.2. CONTINGENCY PLANNING COORDINATOR

The CPC performs the following duties:

- Develops and documents the ISCP under direction of the CPD
- Uses the BIA to prioritize recovery of components
- Updates the ISCP annually
- Ensures that annual ISCP training is conducted
- Facilitates periodic ISCP testing exercises
- Distributes copies of the plan to team members
- Authorizes travel and housing arrangements for team members
- Manages and monitors the overall recovery process
- Leads the contingency response effort once the plan has been activated
- Advises the Procurement and Logistics Coordinator on whether to order new equipment
- Receives updates and status reports from team members
- Sends out communications about the recovery
- Advises the CPD on status as necessary
- Designates key personnel

2.5.3. OUTAGE AND DAMAGE ASSESSMENT LEAD (ODAL)

The ODAL performs the following duties:

- Determines if there has been loss of life or injuries
- Assesses the extent of damage to the facilities and the information systems
- Estimates the time to recover operations
- Determines accessibility to facility, building, offices, and work areas
- Assesses the need for and adequacy of physical security/guards
- Advises the Security Coordinator that physical security/guards are required
- Identifies salvageable hardware
- Maintains a log/record of all salvageable equipment
- Supports the cleanup of the data center following an incident
- Develops and maintains a Damage Assessment Plan
- Estimates levels of outside assistance required
- Reports updates, status, and recommendations to the CPC
- Designates key personnel

2.5.4. HARDWARE RECOVERY TEAM

The hardware recovery team performs the following duties:

- Installs hardware and connects power
- Runs cables and wiring as necessary

- Makes arrangements to move salvageable hardware to other locations as necessary
- Ensures electrical panels are operational
- Ensures that fire suppression system is operational
- Communicates with hardware vendors as needed (Appendix B)
- Creates log of missing and required hardware
- Advises the PLC if new hardware should be purchased
- Connects network cables
- Connects wireless access points

2.5.5. SOFTWARE RECOVERY TEAM

The software recovery team performs the following duties:

- Installs software on all systems at alternate site
- Performs live migrations to alternate site prior to predictable disasters and outages
- Installs servers in the order described in the BIA (Appendix L)
- Communicate with software vendors as needed (Appendix B)
- Advises the PLC if new software needs to be purchased
- Creates log of software installation problems
- Restore systems from most current backup media
- Maintains current system software configuration information in an off-site storage facility

2.5.6. TELECOMMUNICATIONS TEAM

The Telecomm team performs the following duties:

- Assesses the need for alternative communications
- Communicates Internet connectivity requirements with providers
- Communicates with telephone vendors as needed
- Establishes communications between the alternate site and the users
- Coordinates transportation of salvageable telecomm equipment to the alternative site
- Plans for procuring new hardware and telecommunication equipment
- Advises the PLC if new equipment needs to be purchased
- Retrieves communications configuration from the off-site storage facility
- Plans, coordinates and installs communication equipment as needed at the alternate site
- Maintains plan for installing and configuring VOIP
- Maintains current telecommunications configuration information at off-site storage facility.

2.5.7. PROCUREMENT AND LOGISTICS COORDINATOR (PLC)

The PLC performs the following duties:

- Procures new equipment and supplies as necessary
- Prepares, coordinates, and obtains approval for all procurement requests
- Authorizes purchases up to <$ amount> for recovery operations
- Ensures that equipment and supplies are delivered to locations
- Coordinates deliveries
- Updates the CPC with status
- Works with the CPC to provide transportation for staff as needed
- Ensures details of administering emergency funds expenditures are known.
- Processes requests for payment of all invoices related to the incident
- Arranging for travel and lodging of staff to the alternate site as needed
- Procures telephone equipment and leased lines as needed
- Procures alternate communications for teams as needed.

2.5.8. SECURITY COORDINATOR

The Security Coordinator performs the following duties:

- Provides training for employees in facility emergency procedures and measures
- Provides physical security, access control, and safety measures to support recovery effort
- Cordons off the facility including offices to restrict unauthorized access
- Coordinates with the building management and the CPC for authorized personnel access
- Coordinates and manages additional physical security/guards as needed
- Acts as a liaison with emergency personnel, such as fire and police departments
- Provides assistance to officials in investigating the damaged facility/site
- Ensures that data room/center at alternate site has locks (access controls) on the doors
- Coordinates and secures the transportation of files, reports, and equipment in coordination with the CPC.

2.5.9. PLAN DISTRIBUTION AND AVAILABILITY

During a disaster situation, the availability of the contingency plan is essential to the success of the restoration efforts. The Contingency Plan Team has immediate access to the plan upon notification of an emergency. The Contingency Plan Coordinator ensures that a copy of the most current version of the Contingency Plan is maintained at the **<Cloud Service Provider's>** facility. This plan has been distributed to all personnel listed in Appendix A.

Contingency Plan Team members are obligated to inform the Contingency Planning Coordinator, if and when, they no longer require a copy of the plan. In addition, each recipient of the plan is obligated to return or destroy any portion of the plan that is no longer needed and upon termination from **<Cloud Service Provider>**.

2.5.10. LINE OF SUCCESSION/ALTERNATES ROLES

The **<Cloud Service Provider>** sets forth an order of succession, in coordination with the order set forth by the organization to ensure that decision-making authority for the **<Information System Name>** ISCP is uninterrupted.
In order to preserve the continuity of operations, individuals designated as key personnel have been assigned an individual who can assume the key personnel's position if the key personnel is not able to perform their duties. Alternate key personnel are named in a line of succession and are notified and trained to assume their alternate role, should the need arise. The line of succession for key personnel can be found in Appendix A.

3. ACTIVATION AND NOTIFICATION

The activation and notification phase defines initial actions taken once a **<Information System Name>** disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP.

At the completion of the Activation and Notification Phase, key **<Information System Name>** ISCP staff will be prepared to perform recovery measures to restore system functions.

3.1. ACTIVATION CRITERIA AND PROCEDURE

The **<Information System Name>** ISCP may be activated if one or more of the following criteria are met:

1. The type of outage indicates **<Information System Name>** will be down for more than **RTO hours>**
2. The facility housing **<Information System Name>** is damaged and may not be available within **<RTO hours>**
3. Other criteria, as appropriate.

Personnel/roles listed in Table 3-1 are authorized to activate the ISCP.

Name	Title and ISCP Role	Contact Information

Table 3-1 Personnel Authorized to Activate the ISCP

3.2. NOTIFICATION INSTRUCTIONS

Instruction: Describe established notifications procedures. Notification procedures must include who makes the initial notifications, the sequence in which personnel are notified and the method of notification (e.g., email blast, call tree, text messaging, automated notification system, etc.).

Contact information for key personnel is located in Appendix A.

3.3. OUTAGE ASSESSMENT

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by **<role name>**. Assessment results are provided to the Contingency Planning Coordinator to assist in the coordination of the recovery effort.

Instruction: Outline detailed procedures to include how to determine the cause of the outage; identification of potential for additional disruption or damage; assessment of affected physical area(s); and determination of the physical infrastructure status, IS equipment functionality, and inventory. Procedures must include notation of items that will be needed to be replaced and estimated time to restore service to normal operations.

4. RECOVERY

The recovery phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the recovery phase, **<Information System Name>** will be functional and capable of performing the functions identified in Section 4.1 of the plan.

4.1. SEQUENCE OF RECOVERY OPERATIONS

The following activities occur during recovery of **<Information System Name>**:

Instruction: Modify the following list as appropriate for the system recovery strategy.

1. Identify recovery location (if not at original location)
2. Identify required resources to perform recovery procedures
3. Retrieve backup and system installation media
4. Recover hardware and operating system (if required)
5. Recover system from backup and system installation media
6. Implement transaction recovery for systems that are transaction-based.

4.2. RECOVERY PROCEDURES

The following procedures are provided for recovery of **<Information System Name>** at the original or established alternate location. Recovery procedures are outlined per team and must be executed in the sequence presented to maintain an efficient recovery effort.

Instruction: Provide general procedures for the recovery of the system from backup media. Specific keystroke-level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix must be included in this section. Teams or persons responsible for each procedure must be identified.

4.3. RECOVERY ESCALATION NOTICES/AWARENESS

Notifications during recovery include problem escalation to leadership and status awareness to system owners and users. This section describes the procedures for handling escalation notices that define and describe the events, thresholds, or other types of triggers that may require additional action.

Instruction: Provide appropriate procedures for escalation notices during the recovery efforts. Teams or persons responsible for each escalation/awareness procedure must be identified.

5. RECONSTITUTION

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: (1) validating successful reconstitution and (2) deactivation of the plan.

Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

5.1. DATA VALIDATION TESTING

Validation data testing is the process of testing and validating data to ensure that data files or databases have been recovered completely at the permanent location.

Instruction: Describe procedures for testing and validation of data to ensure that data is correct and up to date as of the last available backup. Teams or persons responsible for each procedure must be identified. An example of a validation data test for a moderate-impact system would be to compare a database audit log to the recovered database to make sure all transactions were properly updated. Detailed data test procedures may be provided in Appendix E, System Validation Test Plan.

5.2. FUNCTIONAL VALIDATION TESTING

Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

Instruction: Describe procedures for testing and validation functional and operational aspects of the system.

5.3. RECOVERY DECLARATION

Upon successfully completing testing and validation, the **<role name>** will formally declare recovery efforts complete, and that **<Information System Name>** is in normal operations. **<Information System Name>** business and technical POCs will be notified

of the declaration by the Contingency Plan Coordinator. The recovery declaration statement notifies the Contingency Plan Team and executive management that the **<Information System Name>** has returned to normal operations.

5.4. USER NOTIFICATION

After the recovery declaration statement is made, notifications are sent to users and customers. Notifications to customers are made in accordance with predetermined notification procedures.

Instruction: Describe the notification procedures. Ensure that the procedures described are consistent with Service Level Agreements and contracts.

5.5. CLEANUP

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

Instruction: Describe cleanup procedures and tasks including cleanup roles and responsibilities. Insert cleanup responsibilities in Table 5-1. Add additional rows as needed.

Role	Cleanup Responsibilities

Table 5-1 Cleanup Roles and Responsibilities

5.6. RETURNING BACKUP MEDIA

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures must be followed to return backup and installation media to its offsite data storage location.

Instruction: Provide procedures for returning retrieved backup or installation media to its offsite data storage location. This may include proper logging and packaging of backup and installation media, preparing for transportation, and validating that media is securely stored at the offsite location.

5.7. BACKING UP RESTORED SYSTEMS

As soon as reasonable following recovery, the system must be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:

Instruction: Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period.

5.8. EVENT DOCUMENTATION

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort. Information on lessons learned must be included in the annual update to the ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery event.

Instruction: Provide details about the types of information each ISCP team member is required to provide for the purpose of updating the ISCP. Types of documentation that must be generated and collected after a recovery operation include: activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities); functionality and data testing results; lessons learned documentation; and an After Action Report.

Role Name	Documentation Responsibility
	Activity log
	Functionality and data testing results
	Lessons learned
	After Action Report

Table 5-2 Event Documentation Responsibility

6. CONTINGENCY PLAN TESTING

Contingency Plan operational tests of the **<Information System Name>** are performed annually. A Contingency Plan Test Report is documented after each annual test. A template for the Contingency Plan Test Report is found in Appendix F.

Appendix A – Key Personnel and Team Member Contact List

Instruction: All key personnel (and alternates) and Contingency Plan Team members designated in section 2.5 must be noted on this contact list. The ISCP must be distributed to everyone on this list.

Role	Name and Home Address	Email	Phone
Contingency Plan Director			Primary: Alternate:
Alternate Contingency Plan Director			Primary: Alternate:
Contingency Plan Coordinator			Primary: Alternate:
Alternate Contingency Plan Coordinator			Primary: Alternate:
Outage and Damage Assessment Lead			Primary: Alternate:
Alternate Outage and Damage Assessment Lead			Primary: Alternate:
Procurement and Logistics Coordinator			Primary: Alternate:
Alternate Procurement and Logistics Coordinator			Primary: Alternate:

Appendix B – Vendor Contact List

Vendor	Product or Service License #, Contract #, Account #, or SLA	Phone
		Primary: Alternate:
		Primary: Alternate:
		Primary: Alternate:
		Primary: Alternate:
		Primary: Alternate:
		Primary: Alternate:

Appendix C.1 – Alternate Storage Site Information

Storage Site	
Address of alternate storage site	
Distance from primary facility	
Is alternate storage facility owned by the organization or is a third-party storage provider?	
Points of contact at alternate storage location	
Delivery schedule and procedures for packaging media for delivery to alternate storage facility	
Procedures for retrieving media from the alternate storage facility	
Names and contact information for those persons authorized to retrieve media	
Potential accessibility problems to the alternate storage site in the event of a widespread disruption or disaster (e.g. roads that might be closed, anticipate traffic)	
Mitigation steps to access alternate storage site in the event of a widespread disruption or disaster	
Types of data located at alternate storage site, including databases, application software, operating systems, and other critical information system software	

Appendix C.2 – Alternate Processing Site Information

Alternate Processing Site	
Address	
Distance from primary facility	
Alternate processing site is owned by the organization or is a third-party site provider	
Point of Contact	
Procedures for accessing and using the alternate processing site, and access security features of alternate processing site	
Names and contact information for those persons authorized to go to alternate processing site	
Type of Site (from Table 2-4)	
Mitigation steps to access alternate processing site in the event of a widespread disruption or disaster	

Appendix C.3 – Alternate Telecommunications Provisions

Alternate Telecommunications	
Name and contact information of alternate telecommunications vendors by priority	
Agreements currently in place with alternate communications vendors	
Contracted capacity of alternate telecommunications	
Names and contact information of individuals authorized to implement or use alternate telecommunications	

Appendix D – Alternate Processing Procedures

Instruction: This section must identify any alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed, or queuing of data input.

Appendix E – System Validation Test Plan

Instruction: Describe the system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users. The System Validation Test Plan may include the regression or functionality testing conducted prior to implementation of a system upgrade or change. Edit (or replace) the sample validation test plan provided to reflect the actual validation test plan for the system.

Procedure	Expected Results	Actual Results	Successful?	Performed by
At the Command Prompt, type in sys name	System Log-in Screen appears			
Log-in as user test user, using password test pass	Initial Screen with Main Menu shows			
From menu, select 5-Generate Report	Report Generation Screen shows			
Select Current Date Report Select Weekly Select To Screen	Report is generated on screen with last successful transaction included			
Select Close	Report Generation Screen Shows			
Select Return to Main Menu	Initial Screen with Main Menu shows			
Select Log-Off	Log-in Screen appears			

Appendix F – Contingency Plan Test Report

Instruction: This section must include a summary of the last Contingency Plan Test. The actual procedures used to test the plan must be described in Section 6, not here.

Test Information	Description
Name of Test	
System Name	
Date of Test	
Team Test Lead and Point of Contact	
Location Where Conducted	
Participants	
Components	
Assumptions	
Objectives	Assess effectiveness of system recovery at alternate site Assess effectiveness of coordination among recovery teams Assess systems functionality using alternate equipment Assess performance of alternate equipment Assess effectiveness of procedures Assess effectiveness of notification procedures
Methodology	
Activities and Results (Action, Expected Results, Actual Results)	
Post Test Action Items	
Lessons Learned and Analysis of Test	
Recommended Changes to Contingency Plan Based on Test Outcomes	

Appendix G – Diagrams

Instruction: Insert network diagrams, data flow diagrams, and any relevant component diagrams here. All of the diagrams used must be consistent with those found in the System Security Plan.

Appendix H – Hardware and Software Inventory

Instruction: Insert a hardware and software inventory here. The inventory must be consistent with the one found in the System Security Plan.

Appendix I – System Interconnections

Instruction: Provide a system Interconnection Table which must be consistent with the Interconnections Table found in the System Security Plan. The Interconnections Table from the System Security Plan can be copied and pasted into this Appendix.

Appendix J – Test and Maintenance Schedule

Instruction: All ISCPs must be reviewed and tested at least annually or whenever there is a significant change to the system. Provide information and a schedule for the testing of the system. For moderate-impact systems, a yearly functional test is required.

Appendix K – Associated Plans and Procedures

Instruction: ISCPs for other systems that either interconnect or support the system must be identified in this Appendix. The most current version of the ISCP, location of ISCP, and primary point of contact (such as the ISCP Coordinator) must be noted.

System Name	Plan Name

Appendix L – Business Impact Analysis

Instruction: Insert Business Impact Analysis here. Please see NIST SP 800-34, Revision 1 for more information on how to conduct a Business Impact Analysis.