|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | FedRAMP® System Security Plan (SSP) Appendix G: Information System Contingency Plan (ISCP) Template  for <Insert CSP Name>  <Insert CSO Name>  <Insert Version X.X>  <Insert MM/DD/YYYY> | |  |
|
|  |  | |  |
|  |  | info@fedramp.gov  fedramp.gov |  |

TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 06/6/2014 | 2.1 | All | Major revision for SP 800-53 Revision 4. Includes new template and formatting changes. | FedRAMP |
| 05/18/2016 | 3.0 |  | Reformatted to FedRAMP Document Standard, added repeated text schema and content fields to tables, revised cover page, corrected references from IT Contingency Plan to Information System (IS), changed document designation to Controlled Unclassified Information (CUI), added instruction to complete 15.6 Attachment 6 - Revision History in the System Security Plan, removed front matter section How This Document is Organized, revised Sections 1.5 and 1.6, added instruction to Section 2.1 and Section 5.1, added introductions to appendices. | FedRAMP |
| 09/30/2016 | 3.1 |  | Removed Acronyms and referenced FedRAMP Master Acronyms and Glossary resource document | FedRAMP |
| 10/21/2016 | 3.2 |  | Appendix I - HW and SW Inventory -Instructions reference SSP Attachment 13 – Inventory | FedRAMP |
| 03/9/2017 | 3.3 |  | Renamed document from "FedRAMP Information System Contingency Plan Template" to "SSP ATTACHMENT 6 - FedRAMP Information System Contingency Plan (ISCP) Template " | FedRAMP |
| 06/06/2017 | 3.3 |  | Updated logo | FedRAMP |
| 06/30/2023 | 4.0 | All | Updated to align with the FedRAMP SSP template and remove outdated references. | FedRAMP |
| 12/06/2024 | 5.0 | All | Updated to align with OMB Memo M-24-15 and remove PMO references | FedRAMP |

**How to contact us**

For questions about FedRAMP, or for questions about this document including how to use it, contact [info@FedRAMP.gov.](mailto:info@FedRAMP.gov)

For more information about FedRAMP, see [www.FedRAMP.gov](http://www.fedramp.gov).

Delete this Template Revision History page and all other instructional text from your final version of this document.

Prepared by

|  |  |
| --- | --- |
| Identification of Organization that Prepared this Document | |
| **Organization Name** | <Enter Company/Organization> |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter City, State, and Zip Code> |

Prepared for

|  |  |
| --- | --- |
| Identification of Cloud Service Provider | |
| **Organization Name** | <Enter Company/Organization> |
| **Street Address** | <Enter Street Address> |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter City, State, and Zip Code> |

Document Revision History

Complete for 800-53 Revision 5 the Appendix G: Information System Contingency Plan (ISCP) Revision History. Detail specific changes in the table below.

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

TABLE OF CONTENTS

[1 Introduction and Purpose 7](#_Toc184298571)

[1.1 Applicable Laws and Regulations 7](#_Toc184298572)

[1.2 FedRAMP Requirements and Guidance 7](#_Toc184298573)

[1.3 <Insert CSO Name> and Identifier 8](#_Toc184298574)

[1.4 Scope 8](#_Toc184298575)

[1.5 Assumptions 9](#_Toc184298576)

[2 Concept of Operations 10](#_Toc184298577)

[2.1 System Description 10](#_Toc184298578)

[2.2 Three Phases 10](#_Toc184298579)

[2.3 Data Backup Readiness Information 11](#_Toc184298580)

[2.4 Site Readiness Information 13](#_Toc184298581)

[2.5 Roles and Responsibilities 14](#_Toc184298582)

[3 Activation and Notification 19](#_Toc184298583)

[3.1 Activation Criteria and Procedure 19](#_Toc184298584)

[3.2 Notification Instructions 20](#_Toc184298585)

[3.3 Outage Assessment 20](#_Toc184298586)

[4 Recovery 20](#_Toc184298587)

[4.1 Sequence of Recovery Operations 21](#_Toc184298588)

[4.2 Recovery Procedures 21](#_Toc184298589)

[4.3 Recovery Escalation Notices/Awareness 22](#_Toc184298590)

[5 Reconstitution 22](#_Toc184298591)

[5.1 Data Validation Testing 22](#_Toc184298592)

[5.2 Functional Validation Testing 23](#_Toc184298593)

[5.3 Recovery Declaration 23](#_Toc184298594)

[5.4 User Notification 23](#_Toc184298595)

[5.5 Cleanup 24](#_Toc184298596)

[5.6 Returning Backup Media 24](#_Toc184298597)

[5.7 Backing-Up Restored Systems 25](#_Toc184298598)

[5.8 Event Documentation 25](#_Toc184298599)

[6 Contingency Plan Testing 26](#_Toc184298600)

[Appendix A Key Personnel and Team Member Contact List 27](#_Toc184298601)

[Appendix B Vendor Contact List 28](#_Toc184298602)

[Appendix C Alternate Storage, Processing and Provisions 29](#_Toc184298603)

[Appendix D Alternate Processing Procedures 32](#_Toc184298604)

[Appendix E System Validation Test Plan 32](#_Toc184298605)

[Appendix F Contingency Plan Test Report 33](#_Toc184298606)

[Appendix G Diagrams 35](#_Toc184298607)

[Appendix H Hardware and Software Inventory 35](#_Toc184298608)

[Appendix I System Interconnections with Other Services 36](#_Toc184298609)

[Appendix J Test and Maintenance Schedule 36](#_Toc184298610)

[Appendix K Associated Plans and Procedures 37](#_Toc184298611)

[Appendix L Business Impact Analysis 37](#_Toc184298612)

CONTINGENCY PLAN APPROVALS

|  |
| --- |
| ***Instructions:*** |
| *Add or remove signature boxes, as needed. Digital or wet/physical signatures are permitted.*  Delete this and all other instructional text from your final version of this document. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | | | | |
|  | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | | | | |
|  | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | |  | | |

# Introduction and Purpose

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

One of the goals of an ISCP 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 <Insert CSO Name> components to 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.

## Applicable Laws and Regulations

A summary of <Insert CSO Name>-specific laws and regulations are available in the System Security Plan (SSP), Appendix L, <Insert CSO Name>-specific Required Laws and Regulations.

## FedRAMP Requirements and Guidance

All FedRAMP documents are available at [www.fedramp.gov](https://www.fedramp.gov/)

* FedRAMP Incident Communications Procedure
* FedRAMP Continuous Monitoring Strategy Guide

## <Insert CSO Name> and Identifier

This ISCP applies to the <Insert CSO Name> (Information System Abbreviation), which has a unique identifier as noted in Table 1.3 <Insert CSO Name> and Title.

Table 1.3 <Insert CSO Name> and Title

|  |  |  |
| --- | --- | --- |
| Unique Identifier | Cloud Service Offering Name | Information System Abbreviation |
| Enter FedRAMP Application Number (This is the CSO Unique FedRAMP ID.) | <Insert CSO Name> | ISA |

## Scope

This ISCP has been developed for <Insert CSO Name>, which is classified as a <specify impact level> 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 <specify level> impact system and are designed to recover the CSO within Recovery Time Objective (RTO) <Enter Number> hours. The replacement or purchase of new equipment, short-term disruptions lasting less than <Enter Number>, or loss of data at the primary facility or at the user-desktop levels is outside the scope of this plan.

|  |
| --- |
| ***Instructions:*** |
| *Edit the below list to name other plans and circumstances that are related but are outside the scope of this ISCP.*  Delete this and all other instructional text from your final version of this document. |

Table 1.4 Plans Outside of ISCP Scope below identifies other plans and circumstances that are related but are outside the scope of this ISCP.

Table 1.4 Plans Outside of ISCP Scope

|  |  |
| --- | --- |
| Plan Name | Mission/Purpose |
| Business Continuity Plan (BCP) | Overall recovery and continuity of mission/business operations |
| Continuity of Operations Plan (COOP) | Overall recovery and continuity of mission/business operations |
| The Occupant Emergency Plan (OEP) | Emergency evacuation of personnel |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

## Assumptions

|  |
| --- |
| ***Instructions:*** |
| *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.*  Delete this and all other instructional text from your final version of this document. |

The following assumptions have been made about the <Insert CSO Name>:

* The Uninterruptible Power Supply (UPS) will keep the system up and running after <Enter Number>
* The generators will kick in after <Enter Number> from the time of a power failure.
* Current backups of the application software and data are intact and available at the offsite storage facility in <Enter City, Enter State>.
* The backup storage capability is approved and has been accepted by the Authorizing Official (AO).
* The <Insert CSO Name> is inoperable if it cannot be recovered within <Enter Number> RTO hours.
* Key personnel have been identified and are trained annually in their roles.
* Key personnel are available to activate the ISCP.
* CSP Name defines circumstances that can inhibit recovery and reconstitution to a known state.

# Concept of Operations

This section provides details about the <Insert CSO 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.

## System Description

|  |
| --- |
| ***Instructions:*** |
| *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 – Diagrams.*  *Delete this and all other instructional text from your final version of this document.* |

## Three Phases

This plan has been developed to recover and reconstitute the <Insert CSO 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 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.

## Data Backup Readiness Information

A common understanding of data backup definitions is necessary in order to ensure that data restoration is successful. <Insert CSO Name> recognizes different types of backups, which have different purposes, and those definitions are found in Table 2.1 Backup Types.

Table 2.1 Backup Types

|  |  |
| --- | --- |
| 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. |

The hardware and software components used to create the <Insert CSO Name> backups are noted in Table 2.2 Backup System Components.

Table 2.2 Backup System Components

|  |  |
| --- | --- |
| System/Component | Description |
| Software Used | Click here to enter text. |
| Hardware Used | Click here to enter text. |
| Frequency | Click here to enter text. |
| Backup Type | Click here to enter text. |
| Retention Period | Click here to enter text. |

Table 2.3 Back-Up Storage Location shows the offsite storage facility location of current backups of the <Insert CSO Name> system software and data.

Table 2.3 Back-Up Storage Location

|  |  |
| --- | --- |
| Backup Storage | |
| Site Name | Click here to enter text. |
| Street Address | Click here to enter text. |
| City, State, Zip Code | Click here to enter text. |

Personnel who are authorized to retrieve backups from the offsite storage location, and may authorize the delivery of backups, are noted in Appendix C *–* ­Section 1: Alternate Storage Site Information.

* <Insert CSO Name> 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.

## Site Readiness Information

CSP Name recognizes different types of alternate sites, which are defined in Table 2.4 Alternative Site Types.

Table 2.4 Alternative Site Types

|  |  |
| --- | --- |
| 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. |

Alternate facilities have been established for the <Insert CSO Name> as noted in Table 2.4 Alternative Site Types.

Table 2.5 Primary and Alternative Site Locations

|  |  |  |  |
| --- | --- | --- | --- |
| Designation | Site Name | Site Type | Address |
| Primary Site |  |  |  |
| Alternate Site |  |  |  |
| Alternate Site |  |  |  |

## Roles and Responsibilities

CSP Name establishes multiple roles and responsibilities for responding to outages, disruptions, and disasters for the <Insert CSO 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.

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

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.

### 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

### Contingency Planning Coordinator (CPC)

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

### 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

### Hardware Recovery Team (HRT)

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 – Vendor Contact List)
* Creates log of missing and required hardware
* Advises the PLC if new hardware should be purchased
* Connects network cables
* Connects wireless access points

### Software Recovery Team (SRT)

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 – Business Impact Analysis)
* Communicate with software vendors as needed (Appendix B – Vendor Contact List)
* 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

### Telecommunications Team (TC)

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 telecom 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

### 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 Enter $ 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

### Security Coordinator (SC)

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

### 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 CSP Name’s facility. This plan has been distributed to all personnel listed in Appendix A – Key Personnel and Team Member Contact List.

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 <Insert CSP Name>.

### Line of Succession/Alternates Roles

The <Insert CSP Name> sets forth an order of succession, in coordination with the order set forth by the organization to ensure that decision-making authority for the <Insert CSO 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 – Key Personnel and Team Member Contact List.

# Activation and Notification

The activation and notification phase defines initial actions taken once the <Insert CSO 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 <Insert CSO Name> ISCP staff will be prepared to perform recovery measures to restore system functions.

## Activation Criteria and Procedure

The <Insert CSO Name> ISCP may be activated if one or more of the following criteria are met:

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

Personnel/roles listed in Table 3.1 Personnel Authorized to Activate the ISCP are authorized to activate the ISCP.

Table 3.1 Personnel Authorized to Activate the ISCP

|  |  |  |
| --- | --- | --- |
| Name | Title and ISCP Role | Contact Information |
| Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. |

## Notification Instructions

|  |
| --- |
| ***Instructions:*** |
| *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.).*  *Delete this and all other instructional text from your final version of this document.* |

Contact information for key personnel is located in Appendix A – Key Personnel and Team Member Contact List.

## 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 <Insert Role Name>*.* Assessment results are provided to the Contingency Planning Coordinator to assist in the coordination of the recovery effort.

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

# 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, <Insert CSO Name> will be functional and capable of performing the functions identified in Section 4.1 Sequence of Recovery Operations of the plan.

## Sequence of Recovery Operations

The following activities occur during recovery of <Insert CSO Name>:

|  |
| --- |
| ***Instructions:*** |
| *Modify the following list as appropriate for the system recovery strategy.*  *Delete this and all other instructional text from your final version of this document.* |

* Identification of recovery location (if not at original location)
* Identification of required resources to perform recovery procedures
* Retrieval of backup and system installation media
* Recovery of hardware and operating system (if required)
* Recovery of system from backup and system installation media
* Implementation of transaction recovery for systems that are transaction-based

## Recovery Procedures

The following procedures are provided for recovery of <Insert CSO 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.

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

## 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.

|  |
| --- |
| ***Instructions:*** |
| *Provide appropriate procedures for escalation notices during the recovery efforts. Teams or persons responsible for each escalation/awareness procedure must be identified.*  *Delete this and all other instructional text from your final version of this document.* |

# 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.

## 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.

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

## 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.

|  |
| --- |
| ***Instructions:*** |
| *Describe procedures for testing and validation functional and operational aspects of the system.*  *Delete this and all other instructional text from your final version of this document.* |

## Recovery Declaration

Upon successfully completing testing and validation, the <Insert Role Name> will formally declare recovery efforts complete, and that <Insert CSO Name> is in normal operations. <Insert CSO 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 <Insert CSO Name> has returned to normal operations.

## 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.

|  |
| --- |
| ***Instructions:*** |
| *Describe the notification procedures. Ensure that the procedures described are consistent with Service Level Agreements and contracts.*  *Delete this and all other instructional text from your final version of this document.* |

## 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.

|  |
| --- |
| ***Instructions:*** |
| *Describe cleanup procedures and tasks including cleanup roles and responsibilities. Insert cleanup responsibilities in Table 5.1 Cleanup Roles and Responsibilities. Add additional rows as needed.*  *Delete this and all other instructional text from your final version of this document.* |

Table 5.1 Cleanup Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Cleanup Responsibilities |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

## Returning Backup Media

It is important that all backup and installation media used during recovery be returned to the off-site data storage location.

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

The following procedures must be followed to return backup and installation media to its offsite data storage location: <Inset Procedures>

## Backing-Up Restored Systems

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

|  |
| --- |
| ***Instructions:*** |
| *Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period.*  *Delete this and all other instructional text from your final version of this document.* |

The procedures for conducting a full system backup are: <Inset Procedures>

## 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.

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

Table 5.2 Event Documentation Responsibility lists the responsibility of each ISCP team or person to document their actions during the recovery event.

Table 5.2 Event Documentation Responsibility

|  |  |
| --- | --- |
| Role Name | Documentation Responsibility |
| Click here to enter text. | Activity log |
| Click here to enter text. | Functionality and data testing results |
| Click here to enter text. | Lessons learned |
| Click here to enter text. | After Action Report |

# Contingency Plan Testing

Contingency Plan operational tests of the <Insert CSO 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 – Contingency Plan Test Report.

1. Key Personnel and Team Member Contact List

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

Table A.1 Key Personnel and Team Member Contact List includes Contingency Plan Team members designated in Section 2.5 Roles and Responsibilities and the ISCP has been distributed to everyone in this list.

Table A.1 Key Personnel and Team Member Contact List

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name and Home Address | Email | Phone |
| Contingency Plan Director | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Alternate Contingency Plan Director | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Contingency Plan Coordinator | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Alternate Contingency Plan Coordinator | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Outage and Damage Assessment Lead | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Alternate Outage and Damage Assessment Lead | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Procurement and Logistics Coordinator | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Alternate Procurement and Logistics Coordinator | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |

1. Vendor Contact List

Table B.1 Vendor Contact List includes the vendors associated with the ISCP.

Table B.1 Vendor Contact List

|  |  |  |
| --- | --- | --- |
| Vendor | Product or Service License #, Contract #, Account #, or SLA | Phone |
| Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |
| Click here to enter text. | Click here to enter text. | Primary: Primary Phone.  Alternate: Secondary Phone |

1. Alternate Storage, Processing and Provisions

Section 1: Alternate Storage Site Information

Table C.1 Alternate Storage Site Information lists the alternative site location and details about schedules, data types, and contacts.

Table C.1 Alternate Storage Site Information

|  |  |
| --- | --- |
| Storage Site | |
| Address of alternate storage site | Click here to enter text. |
| Distance from primary facility | Click here to enter text. |
| Is the alternate storage facility owned by the organization or is a third-party storage provider? | Click here to enter text. |
| Points of contact at alternate storage location | Click here to enter text. |
| Delivery schedule and procedures for packaging media for delivery to alternate storage facility | Click here to enter text. |
| Procedures for retrieving media from the alternate storage facility | Click here to enter text. |
| Names and contact information for those persons authorized to retrieve media | Click here to enter text. |
| 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) | Click here to enter text. |
| Mitigation steps to access alternate storage site in the event of a widespread disruption or disaster | Click here to enter text. |
| Types of data located at alternate storage site, including databases, application software, operating systems, and other critical information system software | Click here to enter text. |

Section 2: Alternate Processing Site Information

Table C.2 Alternate Processing Site Information

Table C.2 Alternate Processing Site Information

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

Section 3: Alternate Telecommunications Provisions

Table C.3 Alternate Telecommunications Provisions show the details for the alternate communications vendors, agreements and capacity.

Table C.3 Alternate Telecommunications Provisions

|  |  |
| --- | --- |
| Alternate Telecommunications | |
| Name and contact information of alternate telecommunications vendors by priority | Click here to enter text. |
| Agreements currently in place with alternate communications vendors | Click here to enter text. |
| Contracted capacity of alternate telecommunications | Click here to enter text. |
| Names and contact information of individuals authorized to implement or use alternate telecommunications | Click here to enter text. |

1. Alternate Processing Procedures

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

1. System Validation Test Plan

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

Table E.1 System Validation Test Plan shows the results of testing after the system has recovered and prior to the system being put into full operation.

Table E.1 System Validation Test Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Procedure | Expected Results | Actual Results | Successful? | Performed by |
| At the Command Prompt, type in system 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 |  |  |  |

1. Contingency Plan Test Report

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

Table F.1 Contingency Plan Test Report reflects a summary of the last Contingency Plan Test. The actual procedures used to test the plan are described in Section 6 Contingency Plan Testing.

Table F.1 Contingency Plan Test Report

|  |  |
| --- | --- |
| Test Information | Description |
| Name of Test | Click here to enter text. |
| System Name | Click here to enter text. |
| Date of Test | Click here to enter text. |
| Team Test Lead and Point of Contact | Click here to enter text. |
| Location Where Conducted | Click here to enter text. |
| Participants | Click here to enter text. |
| Components | Click here to enter text. |
| Assumptions | Click here to enter text. |
| Objectives | Select all that apply:   * 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 | Click here to enter text. |
| Activities and Results (Action, Expected Results, Actual Results) | Click here to enter text. |
| Post Test Action Items | Click here to enter text. |
| Lessons Learned and Analysis of Test | Click here to enter text. |
| Recommended Changes to Contingency Plan Based on Test Outcomes | Click here to enter text. |

1. Diagrams

|  |
| --- |
| ***Instructions:*** |
| *It is important that personnel that perform contingency functions (planning, exercise, failover, etc.) have access to the latest authorization boundary, network, and data flow diagrams associated with the service offering. Please ensure access to the System Security Plan by authorized individuals. If there are additional diagrams relevant to contingency planning functions, they may be inserted in this Appendix.*  *Delete this and all other instructional text from your final version of this document.* |

Please refer to <Insert CSO Name> System Security Plan for the service’s authorization boundary, network, and data flow diagrams. Please contact <Insert CSP Designated Point of Contact> for access to the diagrams, as necessary.

1. Hardware and Software Inventory

|  |
| --- |
| ***Instructions:*** |
| *It is important that personnel that perform contingency functions (planning, exercise, failover, etc.) have access to the latest Integrated Inventory Workbook (IIW), which should be maintained and updated monthly by the CSP. Please ensure access to the IIW by authorized individuals.*  *Delete this and all other instructional text from your final version of this document.* |

The <Insert CSO Name> Integrated Inventory Workbook, also provided as Appendix M of the <CSO Name> System Security Plan, provides the complete listing of system components addressed by this Information System Contingency Plan. Please reach to <Insert CSP Designated Point of Contact> for access to the latest version of the Integrated Inventory Workbook, as necessary.

1. System Interconnections with Other Services

|  |
| --- |
| ***Instructions:*** |
| *It is important that personnel that perform contingency functions (planning, exercise, failover, etc.) are aware of all service offering interconnections to both FedRAMP Authorized services/systems and those that lack FedRAMP authorization. This Appendix should reference the applicable SSP sections that address all CSO interconnections for leveraged FedRAMP Authorized services and external systems, services, APIs, and CLIs lacking FedRAMP authorization.*  *Delete this and all other instructional text from your final version of this document.* |

Please refer to the <Insert CSO Name> SSP for information concerning all interconnections to the service, both to FedRAMP Authorized services/systems and those lacking FedRAMP authorization. Please contact <Insert CSP Designated Point of Contact> for access to the SSP, as necessary.

1. Test and Maintenance Schedule

|  |
| --- |
| ***Instructions:*** |
| *All ISCPs must be reviewed and/or tested according to regular schedules. Provide complete information and a schedule for the testing of the system according to all ISCP security control requirements.*  *Delete this and all other instructional text from your final version of this document.* |

1. Associated Plans and Procedures

|  |
| --- |
| ***Instructions:*** |
| *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.*  *Delete this and all other instructional text from your final version of this document.* |

ISCPs for other systems that either interconnect or support the system must be identified in Table K.1 Associated Plans and Procedures.

Table K.1 Associated Plans and Procedures

|  |  |
| --- | --- |
| System Name | Plan Name |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

1. Business Impact Analysis

|  |
| --- |
| ***Instructions:*** |
| *Insert the Business Impact Analysis here. Please see NIST SP 800-34, Revision 1 for more information on how to conduct a Business Impact Analysis.*  *Delete this and all other instructional text from your final version of this document.* |