###### Appendix A—Sample Information System Contingency Plan Templates

Sample templates are provided to address NIST SP 800-53 security controls for each of the three different FIPS 199 impact levels. The templates provided are guides and may be customized and adapted as necessary to best fit the system or organizational requirements for contingency planning. Appendix A.1 can be used for low-impact systems, Appendix A.2 for moderate- impact systems, and Appendix A.3 for high-impact systems.

###### A.1 Sample Template for Low-Impact Systems

**{System name}**

***Security Categorization: Low***

**{Organization Name}**

**Information System Contingency Plan (ISCP)**

**Version [Insert #]**

**[Date]**

**Prepared by**

**[Organization Name] [Street Address]**

**[City, State, and Zip Code]**

**TABLE OF CONTENTS**

**Plan Approval…………………………………………………….………..….……….……A.1-3 1. Introduction ………………………………………………….……..……….…….……..A.1-4**

1.1 Background………..………………………………………….………………..A.1-4

1.2 Scope……..………..…………………………..…….……….……….………..A.1-4

1.3 Assumptions..…….………………………..….……………….……….……...A.1-4

###### 2. Concept of Operations ………………………….……..…………………………..……A.1-5

2.1 System Description………………....……………………………………..…..A.1-5 2.2 Overview of Three Phases..…………………………………………………..A.1-5 2.3 Roles and Responsibilities…….…......……………………………………....A.1-5

###### 3. Activation and Notification………………....………………………..………….……..A.1-6

3.1 Activation Criteria and Procedure ...………………………..………………..A.1-6 3.2 Notification…………………...………………………………..………………..A.1-6 3.3 Outage Assessment…………....…......……………………..………………..A.1-6

###### 4. Recovery……………………….……………....…………………………………………..A.1-7

4.1 Sequence of Recovery Activities ....……………………………..…………..A.1-7 4.2 Recovery Procedures ……...………………………………………..………..A.1-8

4.3 Recovery Escalation Notices/Awareness..……………………………..……A.1-8

###### 5. Reconstitution..……………….……………....………………….………………..……..A.1-8

5.1 Validation Data Testing………...…………………….…….….………….…..A.1-8 5.2 Validation Functionality Testing…........…………….……..…………….…...A.1-8 5.3 Recovery Declaration…………........………………….………………….…..A.1-8

5.4 Notification (users)…. ……...………………………….………………….…..A.1-8

5.5 Cleanup ...……………………...…......……………….………………….……A.1-8

5.6 Data Backup………………...………………………….…………………..…..A.1-8

5.7 Event Documentation…………..…......……………….………………….…..A.1-9

5.8 Deactivation……………………..…......……………….………………….…..A.1-9

###### APPENDICES

**Plan Approval**

*Provide a statement in accordance with the agency’s contingency planning policy to affirm that the ISCP is complete and has been tested sufficiently. The statement should also affirm that the designated authority is responsible for continued maintenance and testing of the ISCP. This statement should be approved and signed by the system designated authority. Space should be provided for the designated authority to sign, along with any other applicable approving signatures. Sample language is provided below:*

As the designated authority for *{system name}*, I hereby certify that the information system contingency plan (ISCP) is complete, and that the information contained in this ISCP provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the system as it relates to the mission of the

*{organization}*, and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this ISCP for *{system name}* will be tested at least annually. This plan was last tested on *{insert exercise date}*; the test, training, and exercise (TT&E) material associated with this test can be found *{TT&E results appendix or location}*. This document will be modified as changes occur and will remain under version control, in accordance with *{organization}*’s contingency planning policy.

*{System Owner Name}* Date

*{System Owner Title}*

###### Introduction

Information systems are vital to {*Organization’s*} mission/business processes; therefore, it is critical that services provided by *{system name}* are able to operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover

{*system name}* quickly and effectively following a service disruption.

###### Background

This *{system name}* ISCP establishes procedures to recover *{system name}* following a disruption. The following recovery plan objectives have been established:

* + - Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
      * ***Activation and Notification phase*** to activate the plan and determine the extent of damage;
      * ***Recovery phase*** to restore *{system name}* operations; and
      * ***Reconstitution phase*** to ensure that *{system name}* is validated through testing and that normal operations are resumed.
    - Identify the activities, resources, and procedures to carry out {*system name}* processing requirements during prolonged interruptions to normal operations.
    - Assign responsibilities to designated *{organization name}* personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
    - Ensure coordination with other personnel responsible for *{organization name}* contingency planning strategies. Ensure coordination with external points of contact and vendors associated with *{system name}* and execution of this plan.

###### Scope

This ISCP has been developed for *{system name}*, which is classified as a low-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 *– Standards for Security Categorization of Federal Information and Information Systems.* Procedures in this ISCP are for Low- Impact systems and designed to recover {*system name}* within *{RTO hours}.* This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than *{RTO hours};* or loss of data at the onsite facility or at the user-desktop levels. As *{system name}* is a low-impact system, alternate data storage and alternate site processing are not required.

###### Assumptions

The following assumptions were used when developing this ISCP:

* + - *{System name}* has been established as a low-impact system, in accordance with *FIPS 199.*
    - Alternate processing sites and offsite storage are not required for this system.
    - The *{system name}* is inoperable and cannot be recovered within *{RTO hours}.*
    - Key *{system name}* personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the *{system name}* Contingency Plan.
    - *Additional assumptions as appropriate.*

The *{system name}* 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 mission/business operations.
    - **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) addresses employee evacuation.
    - *Any additional constraints and associated plans should be added to this list.*

###### Concept of Operations

The Concept of Operations section provides details about *{system name}*, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of {*Organization’s*} personnel during a contingency activation.

###### System Description

*NOTE: Information for this section should be available from the system’s System Security Plan (SSP) and can be copied from the SSP or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.*

###### Overview of Three Phases

This ISCP has been developed to recover and reconstitute the *{system name}* using a three-phased approach. This 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 are:

**Activation and Notification Phase –** Activation of the ISCP occurs after a disruption or outage 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, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

**Recovery Phase –** The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level 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 owners and users.

**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 successful reconstitution and deactivation of the plan.

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

###### Roles and Responsibilities

The ISCP establishes several roles for *{system name}* recovery and reconstitution support*.* Persons or teams assigned ISCP roles have been trained to respond to a contingency event affecting *{system name}.*

*Describe each team and role responsible for executing or supporting system recovery and reconstitution. Include responsibilities for each team/role, leadership roles, and coordination with other recovery and reconstitution teams, as applicable. At a minimum, a role should be established for a system owner or business unit point of contact, a recovery coordinator, and a technical recovery point of contact.*

*Leadership roles should include an ISCP Director, who has overall management responsibility for the plan, and an ISCP Coordinator, who is responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.*

###### Activation and Notification

The Activation and Notification Phase defines initial actions taken once a *{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, *{system name}* ISCP staff will be prepared to perform recovery measures.

###### Activation Criteria and Procedure

The *{system name}* ISCP may be activated if one or more of the following criteria are met:

1. The type of outage indicates *{system name}* will be down for more than *{RTO hours};*
2. The facility housing *{system name}* is damaged and may not be available within *{RTO hours}; and*
3. *Other criteria, as appropriate.*

The following persons or roles may activate the ISCP if one or more of these criteria are met:

*Establish one or more roles that may activate the plan based on activation criteria. Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.*

###### Notification

The first step upon activation of the *{system name}* ISCP is notification of appropriate mission/business and system support personnel. Contact information for appropriate POCs is included in *{Contact List Appendix name}*.

For *{system name}*, the following method and procedure for notifications are used:

*Describe established notification procedures. Notification procedures should include who makes the initial notifications, the sequence in which personnel are notified (e.g., system owner, technical POC, ISCP Coordinator, business unit or user unit POC, and recovery team POC), and the method of notification (e.g., email blast, call tree, automated notification system, etc.).*

###### 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 *{name of recovery team}*. Assessment results are provided to the ISCP Coordinator to assist in the coordination of the recovery of *{system name}.*

*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 should include notation of items that will need to be replaced and estimated time to restore service to normal operations.*

###### 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, *{system name}* will be functional and capable of performing the functions identified in Section 2.1 of this plan.

###### Sequence of Recovery Activities

The following activities occur during recovery of *{system name}:*

*Modify the following list as appropriate for the selected 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); and
5. Recover system from backup and system installation media.

###### Recovery Procedures

The following procedures are provided for recovery of *{system name}* at the original location*.* Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

*Provide general procedures for the recovery of the system from backup media. If an alternate location is part of the recovery strategy, include procedures for recovery to that site. Specific keystroke level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix should be included in this section. Teams or persons responsible for each procedure should be identified.*

###### Recovery Escalation Notices/Awareness

*Provide appropriate procedures for escalation notices during recovery efforts. Notifications during recovery include problem escalation to leadership and status awareness to system owners and users. Teams or persons responsible for each escalation/awareness procedure should be identified.*

###### 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 on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

###### Validation Data 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. The following procedures will be used to determine that the data is complete and current to the last available backup:

*Provide procedures for testing and validation of data to ensure that data is correct and up to date. This section may be combined with the Functionality Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a validation data test for a low-impact system would be to see if the last known complete transaction was updated in the database. Detailed data test procedures may be provided in Appendix E, System Validation Test Plan.*

###### Validation Functionality Testing

Validation functionality testing is the process of verifying that *{system name}* functionality has been tested, and the system is ready to return to normal operations.

*Provide system functionality testing and/or validation procedures to ensure that the system is operating correctly. This section may be combined with the Data Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a functional test for a low-impact system may be logging into the system and running a report or performing a transaction to see if the system is operating correctly. Detailed functionality test procedures may be provided in Appendix E, System Validation Test Plan.*

###### Recovery Declaration

Upon successfully completing testing and validation, the *{system owner}* will formally declare recovery efforts complete, and that *{system name}* is in normal operations. *{System name}* business and technical POCs will be notified of the declaration by the ISCP Coordinator.

###### Notifications (users)

Upon return to normal system operations, {*system name*} users will be notified by *{role}* using

*predetermined notification procedures (e.g., email, broadcast message, phone calls, etc.).*

###### 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.

*Provide any specific cleanup procedures for the system including preferred locations for manuals and documents and returning backup or installation media to its original location.*

###### Data Backup

As soon as reasonable following recovery, the system should 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:

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

###### Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ISCP Coordinator.

*Provide details about the types of information each ISCP team member is required to provide or collect for updating the ISCP with lessons learned. Types of documentation that should be generated and collected after a contingency activation 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*
    - *After Action Report.*

*Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.*

###### Deactivation

Once all activities have been completed and documentation has been updated, the *{system owner}* will formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

###### SUGGESTED APPENDICES

*ISCP appendices included should be based on system and plan requirements. The following appendices are recommended:*

###### APPENDIX A PERSONNEL CONTACT LIST

*Provide contact information for each person with a role or responsibility for activation or implementation of the ISCP, or coordination with the ISCP. For each person listed, at least one office and one non-office contact number is recommended. Note: Information may contain personally identifiable information and should be protected.*

|  |  |  |
| --- | --- | --- |
| *{System name}* **ISCP Key Personnel** | | |
| **Key Personnel** | **Contact Information** | |
| **ISCP Director** | Work | *Insert number* |
| *Insert Name and Title* | Home | *Insert number* |
| *Insert Street Address* | Cellular | *Insert number* |
| *Insert City, State, and Zip Code* | Email | *Insert email address* |
| **ISCP Director – Alternate** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
| **ISCP Coordinator** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
| **ISCP Coordinator – Alternate** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
| **ISCP Team – Team Lead** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |
| **ICSP Team – Team Members** | Work |  |
|  | Home |  |
|  | Cellular |  |
|  | Email |  |

###### APPENDIX B VENDOR CONTACT LIST

*Contact information for all key maintenance or support vendors should be included in this appendix. Contact information, such as emergency phone numbers, contact names, contract numbers, and contractual response and onsite times should be included.*

###### APPENDIX C DETAILED RECOVERY PROCEDURES

*This appendix includes the detailed recovery procedures for the system, which may include items such as:*

* + - *Keystroke-level recovery steps;*
    - *System installation instructions from tape, CD, or other media;*
    - *Required configuration settings or changes;*
    - *Recovery of data from tape and audit logs; and*
    - *Other system recovery procedures, as appropriate.*

*If the system relies totally on another group or system for its recovery and reconstitution (such as a mainframe system), information provided should include contact information and locations of detailed recovery procedures for that supporting system.*

###### APPENDIX D ALTERNATE PROCESSING PROCEDURES

*This section should 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

*This appendix includes 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 data testing and the regression or functionality testing conducted prior to implementation of a system upgrade or change.*

*An example of a system validation test plan:*

Once the system has been recovered, the following steps will be performed to validate system data and functionality:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Procedure** | **Expected Results** | **Actual Results** | **Successful?** | **Performed by** |
| At the Command Prompt, type in sysname | System Log-in Screen appears |  |  |  |
| Log in as user testuser, using password testpass | 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 DIAGRAMS (SYSTEM AND INPUT/OUTPUT)

*NOTE: Information for this section should be available from the system’s System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Include any system architecture, input/output, or other technical or logical diagrams that may be useful in recovering the system. Diagrams may also identify information about interconnection with other systems.*

###### APPENDIX G HARDWARE AND SOFTWARE INVENTORY

*Provide the hardware and software inventory for the system. Inventory information should include type of server or hardware on which the system runs, processors and memory requirements, storage requirements, and any other pertinent details. The software inventory should identify the operating system (including service pack or version levels, and any other applications necessary to operate the system, such as database software).*

###### APPENDIX H INTERCONNECTIONS TABLE

*NOTE: Information for this section should be available from the system’s System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. This appendix includes information on other systems that directly interconnect or exchange information with the system. Interconnection information should include the type of connection, information transferred, and contact person for that system.*

*If the system does not have any direct interconnections, then this appendix may be removed, or the following statement may be used:*

*{System name}* does not directly interconnect with any other systems.

###### APPENDIX I TEST AND MAINTENANCE SCHEDULE

*All ISCPs should be reviewed and tested at the organization defined frequency (e.g. yearly) or whenever there is a significant change to the system. Provide information and a schedule for the testing of the system. For low-impact systems, a yearly tabletop exercise is sufficient. The tabletop exercise should include all ISCP points of contact, and be conducted by an outside or impartial observer. A formal test plan is developed prior to the tabletop, and an exercise and questions are developed to include key sections of the ISCP, including a walk-through of the following:*

* *Notification procedures;*
* *System recovery on an alternate platform from backup media;*
* *Internal and external connectivity; and*
* *Reconstitution procedures.*

*Results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the ISCP.*

*The following is a sample of a yearly test and maintenance schedule for a low-impact system:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step | Date Due by | Responsible Party | Date Scheduled | Date Held |
| Identify tabletop facilitator. | April 1 | ISCP Coordinator |  |  |
| Develop tabletop test plan. | May 1 | Tabletop Facilitator |  |  |
| Invite participants. | May 10 | Tabletop Facilitator |  |  |
| Conduct tabletop test. | May 31 | Facilitator, ISCP Coordinator, POCs |  |  |
| Finalize after action report and lessons learned. | June 10 | ISCP Coordinator |  |  |
| Update ISCP based on lessons learned. | June 30 | ISCP Coordinator |  |  |
| Approve and distribute updated version of ISCP. | July 15 | ISCP Director, ISCP Coordinator |  |  |

###### APPENDIX J ASSOCIATED PLANS AND PROCEDURES

*NOTE: Information for this section should be available from the system’s System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. ISCPs for other systems that either interconnect or support the system should 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) should be noted.*

###### APPENDIX K BUSINESS IMPACT ANALYSIS

*The Business Impact Analysis results should be included in this appendix.*

###### APPENDIX L DOCUMENT CHANGE PAGE

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

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