CONTINGENCY PLAN

Introduction

The <Program Name> < System Name> Contingency Plan (CP), documents the strategies, personnel, procedures, and resources required to respond to any short or long term interruption to the system.

Scope

This CP has been developed for <System Name> which is classified as a <moderate-low-low> impact system for the three security objectives: confidentiality, integrity, and availability. The procedures in this CP have been developed for a moderate-low-low impact system and are designed to recover the <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.

Note: *RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission/business processes.*

Assumptions

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

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

- The Uninterruptable Power Supply (UPS) will keep the system up and running for <total number of seconds/minutes>.
- The generators will initiate 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 <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 CP.

Roles and Responsibilities

The <System Name> roles and responsibilities for various task assignments and deliverables throughout the contingency planning process are depicted in the table below.

Table 1: Roles and Responsibilities

Roles	Responsibilities
INFORMATION SYSTEM OWNER/PROGRAM MANAGER (ISO/PM) – Disruption Occurs	The responsibilities of the ISO/PM when a disruption occurs are listed but not limited to the following: <enter responsibilities>
SYSTEM ADMINISTRATOR (SA)	The responsibilities of the SA are listed but not limited to the following: <enter responsibilities>
PROGRAM SECURTY OFFICER (PSO)	The responsibilities of the PSO are listed but not limited to the following: <enter responsibilities>
INFORMATION SYSTEM SECURITY MANAGER/INFORMATION SYSTEM SECURITY OFFICER (ISSM/ISSO)	The responsibilities of the ISSM/ISSO are listed but not limited to the following: <enter responsibilities>

System Description and Architecture

Instruction: *It is necessary to include a general description of the system covered in the CP. The description should include the Information Technology (IT) system architecture, locations, and any other important technical considerations.*

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

Contingency Plan Phases

This plan has been developed to recover and reconstitute the <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 CP 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 CP is activated, the system stakeholders are notified of a possible long-term outage, and a thorough outage assessment is performed for the 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.

Data Backup Readiness Information

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

Table 2: Backup System Components

System/Components	Description
Software Used	
Hardware Used	
Date of Last Backup	
Backup Type (Full, Differential, Incremental)	

Alternate Site/Backup Storage Information

Alternate facilities have been established for backup storage and/or restoration of the <System Name> as noted in Table 3. Current backups of the system configuration, software and data are intact and available at the alternate storage facility.

Table 3: Primary and Alternate Site Locations

Designation	Site Name	Site Type (Hot, Cold, Warm, Mirrored)	Address
Primary Site			
Alternate Site			
Alternate Site			

Activation and Notification

The activation and notification phase defines initial actions taken once a disruption has been detected or appears to be imminent. The RTO defines the maximum amount of time that the information system can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the maximum tolerable downtime. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the maximum tolerable downtime. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the CP. At the completion of the Activation and Notification Phase, key CP staff will be prepared to perform recovery measures to restore system functions.

Activation Criteria

The CP may be activated if one or more of the following criteria are met:

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

Recovery

The recovery phase provides formal recovery operations that begin after the CP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate individuals 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 essential functions.

Sequence of Recovery Operations

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

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

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

Recovery Procedures

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 should be included in this section. Teams or persons responsible for each procedure should be identified.*

The following procedures are provided for recovery of <System Name> at the original or established alternate location. Recovery procedures should be executed in the sequence presented to maintain an efficient recovery effort.

Instruction: *Describe recovery procedures.*

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.

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

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 should 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.*

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.

Functional Validation Testing

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

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

Recovery Declaration

Upon successfully completing testing and validation, the <role name> will formally declare recovery efforts complete, and that <System Name> is in normal operations. <System Name> users and technical POCs will be notified of the declaration by the <role name>. The recovery declaration statement notifies the stakeholders and management that the <System Name> has returned to normal operations.

Post Reconstitution

Cleanup

Instruction: *Describe cleanup procedures and tasks including cleanup roles and responsibilities. Insert cleanup responsibilities in Table 4. Add additional rows as needed.*

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.

Table 4: Primary Cleanup Roles and Responsibilities

Roles	Cleanup Responsibilities

Backup Procedures

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.*

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

<Enter procedures>

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.*

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:

<Enter procedures>

After Action Reporting

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 should be included in the annual update to the CP. It is the responsibility of each CP team or person to document their actions during the recovery event.

Contingency Plan Testing

Contingency Plan operational tests of the <System Name> are performed **at least annually**. A Contingency Plan Test (CPT) report is documented after each annual test.

Instruction: *Describe the procedures for the annual contingency plan testing. Include a description of the required test environment. Operational tests typically include the following:*

1. *Restore files from backup tapes.*
2. *Verify that backup tapes are stored at designated off-site locations.*
3. *Determine whether data stored on backup tapes is valid and retrievable.*
4. *Perform failover testing.*
5. *Test the UPS to ensure that it operates correctly in the event of a power disruption;*
6. *Test the offsite backup vendor's delivery response timeliness of media during normal daytime hours and during nighttime hours*
7. *Test to ensure that offsite storage vendor only supplies backup tapes to authorized individuals*
8. *Test the generators to ensure that they turn on automatically*
9. *Perform tabletop exercises to test various possible contingency situations*
10. *Perform call tree exercises to ensure that employees can be reached in a timely manner.*

Instruction: *Describe methods used to test CP in this section.*

Contingency Plan Testing Report Template

Instruction: *This section should include a summary of the last Contingency Plan Test.*

Table 5: Contingency Plan Test Summary

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	

Note: The Contingency Plan Template is intended as a guideline. Industry will need to adjust the Contingency Plan to meet their specific requirements and comply with any additional and/or contractual requirements.