State of Ohio
Disaster Recovery Planning Template
For Low Impact Information Technology Systems
(Low Risk DRP Template)

[Agency Name]
[Street Address]
[City, State, and Zip Code]

Table of Contents

Purpose of the Template

Sample templates are provided to address security controls recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 for each of the three different impact levels: low, moderate, and high. This guidance may be customized and adapted as necessary to best fit the agency requirements for information technology disaster recovery planning. This specific plan template is modeled after planning methods recommended for low impact systems, based on NIST SP 800-34.

Italicized text is included throughout this template only to provide further direction or guidance for agencies to use in developing their respective DRPs. This italicized text should be deleted as the template is completed.

I. System Information

{System name}

Security Categorization: Low

{Agency Name}

II. Plan Approval

Provide a statement in accordance with the agency's disaster recovery planning policy to affirm that the DRP is complete and has been tested sufficiently. The statement should affirm that the designated authority is responsible for continued maintenance and testing of the DRP and 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 disaster recovery plan (DRP) is complete, and that the information contained in this DRP 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 *{agency}*, 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 DRP 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 attachment or location}*. This document will be modified as changes occur and will remain under version control, in accordance with *{agency}*'s disaster recovery planning policy.

III. Introduction

Information systems are vital to {*Agency's*} mission and business processes; therefore, it is critical that services provided by *{system name}* are able to operate effectively without excessive interruption. This information system DRP establishes comprehensive procedures to recover {*system name}* quickly and effectively following a service disruption.

A. Background

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

- Maximize the effectiveness of disaster recovery 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 *{agency name}* employee and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other employee responsible for *{agency name}* disaster recovery planning strategies. Ensure coordination with external points of contact and vendors associated with *{system name}* and execution of this plan.

This DRP 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 DRP 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.

B. Assumptions

The following assumptions were used when developing this DRP:

- *{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}* employees have been identified and trained in their emergency response and recovery roles; they are available to activate the *{system name}* Disaster Recovery Plan.
- *Additional assumptions as appropriate.*

C. Scope

The *{system name}* DRP does not apply to the following situations:

- **Overall recovery and continuity of mission/business operations.** The {*Agency's*} overall Continuity of Operations Plan (COOP) addresses continuity of mission essential functions.
- **Emergency evacuation of employee.** The Employee Emergency Response Plan (ERP) addresses employee evacuation.
- *Any additional constraints and associated plans should be added to this list.*

IV. Concept of Operations

This Concept of Operations section provides details about *{system name}*, an overview of the three phases of the DRP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of {*Agency's*} employees during a disaster recovery activation.

A. 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 disaster recovery plan. Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external agencies/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.

B. Overview of Three Phases

This DRP 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:

1. **Activation and Notification Phase –** Activation of the DRP 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 DRP 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.

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 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.

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 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.

C. Roles and Responsibilities

The DRP establishes several roles for *{system name}* recovery and reconstitution support. Persons or teams assigned DRP roles have been trained to respond to a disaster recovery 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 a DRP Manager, who has overall management responsibility for the plan, and a DRP 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.

V. 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 employee, conduct an outage assessment, and activate the DRP. At the completion of

the Activation and Notification Phase, *{system name}* DRP staff will be prepared to perform recovery measures.

A. Activation Criteria and Procedure

The *{system name}* DRP 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}; and*
- *Other criteria, as appropriate.*

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

- *Establish one or more roles that are granted the authority to activate the DRP based on activation criteria listed above. Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.*

B. Notification

The first step upon activation of the *{system name}* DRP is notification of the appropriate business area(s) and system support employee. Contact information for appropriate POCs is included in Attachment A. Employee Emergency Contact List.

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

- *Describe established notification procedures. Notification procedures should include who makes the initial notifications, the sequence in which employee are notified (e.g., system owner, technical POC, DRP 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.).*

C. 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 DRP 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.

VI. Recovery

The Recovery Phase provides formal recovery operations that begin after the DRP has been activated, outage assessments have been completed (if possible), employees 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 V. A. (System Description) of this plan.

A. 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.*

- 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); and
- Recover system from backup and system installation media.

B. 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 attachment. If specific procedures are provided in an attachment, a reference to that attachment should be included in this section. Teams or persons responsible for each procedure should be identified.

C. 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.

VII. 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.

A. 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 Attachment E. System Validation Test Plan.

B. 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 Attachment E. System Validation Test Plan.

C. 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 DRP Coordinator.

D. 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.).*

E. 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 disaster recovery 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.

F. 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.

G. 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 DRP. It is the responsibility of each DRP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the DRP Coordinator.

Provide details about the types of information each DRP team member is required to provide or collect for updating the DRP with lessons learned. Types of documentation that should be generated and collected after DRP 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.

H. Deactivation

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

VIII. Attachments

DRP attachments included should be based on system and plan requirements. Recommended attachments are discussed on the following pages.

- *Attachment A. Employee Emergency Contact List*
- *Attachment B. Vendor Contact List*
- *Attachment C. Detailed Recovery Procedures*
- *Attachment D. Alternate Processing Procedures*
- *Attachment E. System Validation Test Plan*
- *Attachment F. Diagrams (System Input/Output)*
- *Attachment G. Hardware/Software Inventory*
- *Attachment H. Interconnections*
- *Attachment I. Test and Maintenance Schedule*
- *Attachment J. Associated Plans and Procedures*
- *Attachment K. Business Impact Analysis*
- *Attachment L. Record of Changes*

A. Attachment A. Employee Emergency Contact List

Provide contact information for each person with a role or responsibility for activation or implementation of the DRP or coordination with the DRP. 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} **DRP KEY STAFF EMERGENCY CONTACT LIST**		
Key Employee	**Contact Information**	
DRP Manager	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*
(Insert Name), DRP Manager – Alternate	Work	
Home		
Cellular		
Email		
(Insert Name), DRP Coordinator	Work	
Home		
Cellular		
Email		
(Insert Name), DRP Coordinator – Alternate	Work	
Home		
Cellular		
Email		
(Insert Name), DRP Team Lead	Work	
Home		
Cellular		
Email		
(Insert Name), DRP Team Member(s)	Work	
Home		
Cellular		
Email		

B. Attachment B. Vendor Contact List

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

Vendor	Contract #	Contact Name	Phone Number	Required Response Time

C. Attachment C. Detailed Recovery Procedures

This attachment 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.

D. Attachment 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.

E. Attachment E. System Validation Test Plan

This attachment 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			

F. Attachment F. Diagrams (System 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 disaster recovery 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.

G. Attachment G. Hardware/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).

H. Attachment H. Interconnections

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 disaster recovery plan. This attachment 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.

System Name	Type of Connection (Interconnect or Exchange)	Information Transferred	Contact Person

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

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

I. Attachment I. Test and Maintenance Plan

All DRPs should be reviewed and tested at the agency-defined frequency (i.e., annually) 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 DRP 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 DRP, 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 Corrective Action Plans are developed for updating information in the DRP.

Examples of functional tests that may be informed include:

- *All notification and response of key personnel to recovery locations;*
- *Recovery of a server or database from backup media; and/or*
- *Setup and processing from a server at an alternate location.*

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

Step	Date Due	Responsible Party	Date Scheduled	Date Held
Identify tabletop facilitator.	04/01/15	DRP Coordinator	04/01/15	04/01/15
Develop tabletop test plan.	05/01/15	Tabletop Facilitator	05/01/15	05/01/15
Invite participants.	05/10/15	Tabletop Facilitator	05/10/15	05/10/15
Conduct tabletop test.	05/31/15	Facilitator DRP Coordinator POCs	05/31/15	05/31/15
Finalize after action report and lessons learned.	06/10/15	DRP Coordinator	06/10/15	06/10/15
Update DRP based on lessons learned.	06/30/15	DRP Coordinator	06/30/15	06/30/15
Approve and distribute updated version of DRP.	07/15/15	DRP Manager DRP Coordinator	07/15/15	07/15/15

J. Attachment 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 disaster recovery plan. DRPs for other systems that either interconnect or support the system should be identified in this attachment. The most current version of the DRP, location of DRP, and primary point of contact (such as the DRP Coordinator) should be noted.

K. Attachment K. Business Impact Analysis

The Business Impact Analysis results should be included in this attachment.

L. Attachment L. Record of Changes

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

Page No.	Change	Date of Change	Revised by: