USAID
FROM THE AMERICAN PEOPLE

Disaster Recovery Planning Procedures and Guidelines

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mal_060106_cd44

Information System Security
Disaster Recovery Planning Procedures and Guidelines
for System Owners, Information System Security Officers, and System Administrators

1. Introduction

This document defines the procedures and guidelines that you must follow for developing, testing and maintaining a USAID system Disaster Recovery Plan. They are streamlined from the guidance provided in NIST Special Publication 800-34, **Contingency Planning Guide for Information Technology Systems**.

2. Disaster Recovery Planning

Disaster recovery planning consists of deciding in advance what, how, when and who are needed to provide a solution that will sustain critical business functions. The planning process includes steps that identify and document key elements in a successful disaster recovery solution. These steps include the following:

1. Identifying and prioritizing business-critical systems and functions,
2. Identifying business-critical resources and performing impact analysis,
3. Developing a notification plan,
4. Developing a damage assessment plan,
5. Designating a disaster recovery site (if necessary and possible),
6. Developing a plan to recover critical functions at the disaster recovery site, and identifying and documenting security controls, and
7. Designating responsibilities.

Disaster recovery planning is an ongoing, dynamic process that continues throughout the information system's lifecycle. The Disaster Recovery Planning process for System Owners, Information System Security Officers, and System Administrators is depicted in the flow chart in Section 4, below.

For the Missions, disaster recovery planning has practical limits. Usable space may be unavailable, and there may be little or no option for an alternate disaster recovery site. Valid disaster recovery options may be to recover information systems locally, at USAID/W, or there maybe none at all (Mission-in-Exile). Recovery can also be cold, warm, or hot as required by the criticality of the information system and the acceptable outage time.

2.1 Identifying Critical Systems and Functions

Information systems can be very complex, fulfilling many business functions. Your **first step** in disaster recovery planning is to identify and prioritize the business-critical functions, systems, and processes. As a disaster recovery planner, you must obtain input from Executive and Functional Managers to determine each system's criticality.

2.2 Identifying Critical Resources

Your **second step** in disaster recovery planning is to identify the resources that are critical to the information systems that support the functions, systems, and processes that you identified in step one. The critical resources that you identify must include everything necessary to support the critical function, system, or process. Some examples of critical resources are:

- Servers, workstations and peripherals,
- Applications and data,
- Media and output,
- Telecommunications connections,
- Physical infrastructure (e.g., electrical power, environmental controls), and
- Personnel.

As a disaster recovery planner, you must analyze the critical resources identified and determine the impact on information system operations if a given resource is disrupted or damaged. The impact analysis must include allowable outage times, i.e., "How long can USAID afford to be without this resource?" When analyzing the impact, you must also consider the outage effect on dependent systems.

Using the resulting business impact analysis, you must then develop and prioritize strategies for recovery and restoration. For a sample business impact analysis, see **Business Impact Analysis Template**.

2.3 Developing a Notification Plan

Your **third step** is to develop a plan for notifying essential personnel when a disaster occurs or is imminent. The plan must describe the methods USAID uses to notify personnel during business and non-business hours. Prompt notification can reduce the disaster's effects on the information system because you will have time to take mitigating actions.

2.4 Developing a Damage Assessment Plan

Your **fourth step** is to develop a plan for assessing the nature and extent of damage to the system, and determine the extent to activate the Disaster Recovery Plan. Although damage assessment procedures may be unique for each system, you must address the following areas:

- Cause of the outage or interruption,
- Damage to the information system or data,
- Potential for additional disruption or damage,
- Physical infrastructure status,
- Information system inventory and functional status,
- Requirements for repair or replacement, and
- Estimated time to recover or restore.

Disaster Recovery Plan activation criteria (the conditions under which you activate the plan) are unique to each event and you must state them in the plan. You must base criteria on:

- Information system damage,
- Facility damage,
- System criticality, and
- Anticipated disruption length.

2.5 Designate a Disaster Recovery Site

If you must recover a USAID information system at an alternate site, you must follow the guidance in this step. For the Missions, the designation of an alternate disaster recovery site depends upon the choice of disaster recovery options. If you choose to recover at USAID/W or at a Mission-in-Exile, there may be infrastructure or other support which you can use during a disaster. Your duties under disaster recovery planning are to identify these support mechanisms and to validate that they will be available for your use, if needed.

Your **fifth step** is to choose a disaster recovery site where USAID will perform recovery of system operations until restoration is possible. The Disaster Recovery Plan must define the specific site for the contingencies identified within the plan. The following table describes the site types that may be used:

Site Type	Description	Cost	Setup Time
Cold Site	A facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the information system, but no equipment.	Low	Long
Warm Site	Partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status, ready to receive the relocated system.	Medium	Medium
Hot Site	Office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.	Medium/High	Short
Mirrored Site	Fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.	High	None

This table describes types of disaster recovery, costs, and setup times.

You must account for the information system criticality requirements when choosing a disaster recovery site. Some criteria for choosing a site include: compatibility, availability, cost, and setup time. If you choose a mirrored site, then you need to include procedures in your Concept of Operations Plan and your Disaster Recovery Plan to a) make certain that USAID coordinates processing and b) that the two systems remain in-sync.

2.6 Developing a Plan to Recover Critical Functions

Your **sixth step** in disaster recovery planning is to establish how you will recover critical functions. The planning requirements for this step may include procuring and setting up necessary equipment, providing guaranteed safety and transportation for personnel, obtaining backups from storage, etc. You must include the procedures that support these requirements in your Disaster Recovery Plan.

2.7 Designate Responsibilities

Your **seventh step** in disaster recovery planning is to designate responsibility for key activities identified and their duties outlined within the Disaster Recovery Plan. You must make certain that the designated personnel are trained to perform their activities.

3. Implement and Maintain the Disaster Recovery Plan

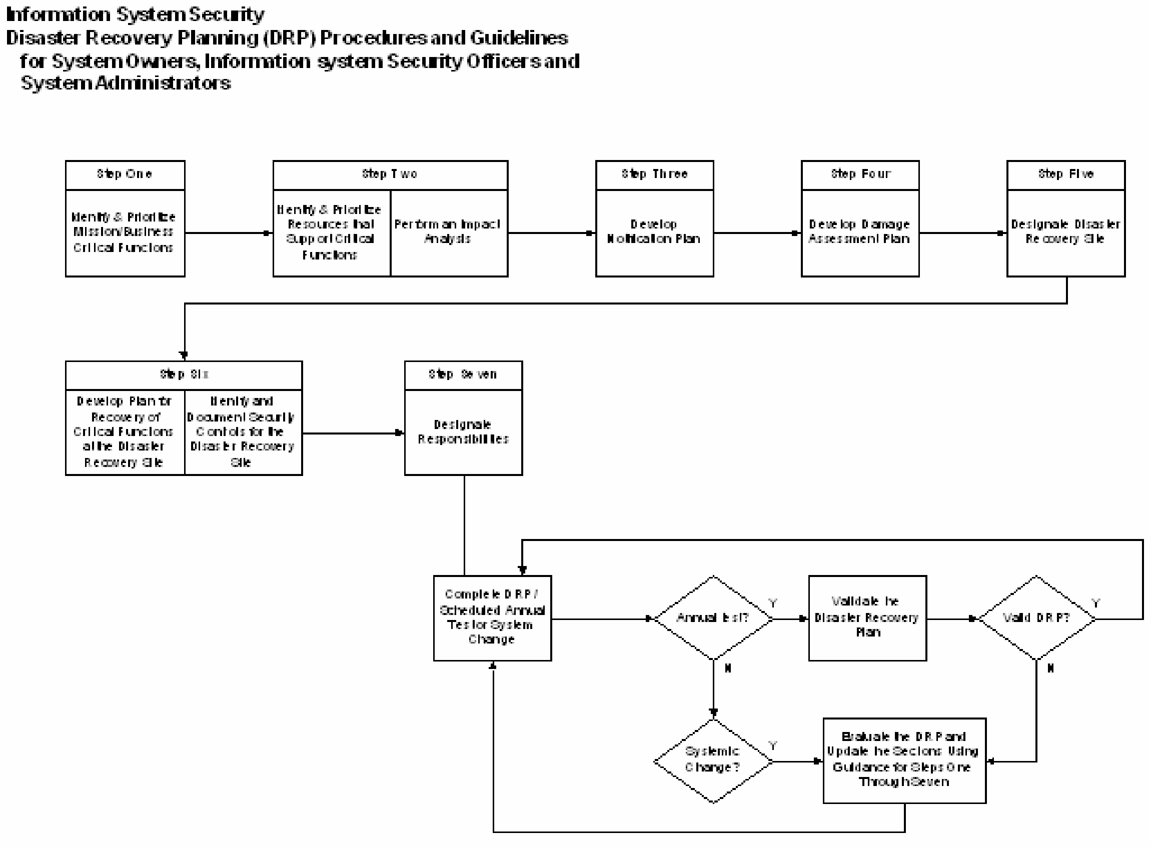
The first seven steps, as taken, populate sections of the Disaster Recovery Plan. Once populated, you must keep the Disaster Recovery Plan up-to-date, and securely store it for use. You must validate the Disaster Recovery Plan annually. Whenever there are changes to your information system, you must update and validate the Disaster Recovery Plan.

When you test and validate the Disaster Recovery Plan, you ***must never disrupt*** normal operation of the information system without the express consent of the System Owner, the CISO, and USAID Executive Management. You must produce and evaluate test reports, and revise the Disaster Recovery Plan, if necessary.

You must submit a copy of the initial DRP to the CISO. When there are subsequent updates, you must submit copies to the CISO. You must submit a **Disaster Recovery Plan Annual Validation Letter** to the CISO at the conclusion of validation testing.

4. Disaster Recovery Planning Flow Chart

The Disaster Recovery Planning process for System Owners, Information System Security Officers, and System Administrators is described in the following flow chart:


Information System Security
Disaster Recovery Planning (DRP) Procedures and Guidelines
for System Owners, Information system Security Officers and
System Administrators
Step One
Identify & Prioritize Mission/Business Critical Functions
Step Two
Identify & Prioritize Resources that Support Critical Functions
Perform an Impact Analysis
Step Three
Develop Notification Plan
Step Four
Develop Damage Assessment Plan
Step Five
Designate Disaster Recovery Site
Step Six
Develop Plan for Recovery of Critical Functions at the Disaster Recovery Site
Identify and Document Security Controls for the Disaster Recovery Site
Step Seven
Designate Responsibilities
Complete DRP / Scheduled Annual Test or System Change
Annual Test?
Y
N
Validate the Disaster Recovery Plan
Valid DRP?
Y
N
Systemic Change?
Y
Evaluate the DRP and Update the Sections Using Guidance for Steps One Through Seven

The above graphic uses standard flow chart symbols to illustrate the steps and decisions involved in Disaster Recover Planning as described in the text of this document.

References

You may use the **Disaster Recovery Plan Template** for all USAID information systems. You can find supplemental guidance in the following documents:

- Federal Preparedness Circular (FPC) 65, **Federal Executive Branch Continuity of Operations**, July 1999.

- NIST Federal Information Processing Standard Publication (FIPS PUB) 87, **Guidelines for ADP Contingency Planning**, March 1981. Which has been superseded by **Special Publication 800-34, Contingency Planning Guide for Information Technology Systems**, June 2002.

- NIST Special Publication 800-12, **An Introduction to Computer Security: The NIST Handbook**, Chapter 11, October 1995.

- Presidential Decision Directive (PDD) 63, **Critical Infrastructure Protection**, May 1998.