# DOCUMENT INFORMATION SHEET

Title: Disaster Recovery Plan

Subject: Name the Plan Subject

Date: [Publish Date]

Author: Author Name

Job Title: What is your job title?

Department: What is your department?

Phone: What is your contact phone number?

Email: What is your contact email?

Version: 1.0 *[tip: Use small increments (1.1., 1.2 etc.) for minor changes and larger increments for major changes (2.0, 3.0, etc.)]*

Status: Choose an item.

Contents

[DOCUMENT INFORMATION SHEET 1](#_Toc392791004)

[DOCUMENT NOTES 4](#_Toc392791005)

[1.0 STATEMENT OF GOALS AND OBJECTIVES 5](#_Toc392791006)

[2.0 PLANNING ASSUMPTIONS 6](#_Toc392791007)

[2.1 Requirements Assumptions 6](#_Toc392791008)

[2.2 Recovery Assumptions 6](#_Toc392791009)

[3.0 PLAN ACTIVATION CRITERIA 7](#_Toc392791010)

[3.1 Plan Activation Criteria 7](#_Toc392791011)

[3.2 Plan Activation Procedures 7](#_Toc392791012)

[4.0 SCENARIOS AND RESPONSE STRATEGIES 8](#_Toc392791013)

[5.0 DISASTER RECOVERY REQUIREMENTS 9](#_Toc392791014)

[5.1 Technology Requirements 9](#_Toc392791015)

[5.2 Operational Requirements 9](#_Toc392791016)

[5.3 Communications Requirements 9](#_Toc392791017)

[5.4 Backup Requirements 10](#_Toc392791018)

[5.5 Documentation Requirements 10](#_Toc392791019)

[5.6 Supplies Requirements 10](#_Toc392791020)

[5.7 Training Requirements 10](#_Toc392791021)

[6.0 DISASTER RECOVERY PROCEDURES 11](#_Toc392791022)

[6.1 Communications Procedures 11](#_Toc392791023)

[6.2 Remote Access Procedures 11](#_Toc392791024)

[6.3 Technical Implementation Procedures 11](#_Toc392791025)

[6.4 Backup and Data Recovery Procedures 11](#_Toc392791026)

[6.5 Temporary Access Procedures 12](#_Toc392791027)

[6.6 Technical Support Procedures 12](#_Toc392791028)

[6.7 Alternative Operating Procedures 12](#_Toc392791029)

[7.0 ROLES AND RESPONSIBILITIES 13](#_Toc392791030)

[7.1 Disaster Recovery Team Mission Statement 13](#_Toc392791031)

[7.2 Organizational Chart 13](#_Toc392791032)

[7.3 Resource Requirements 14](#_Toc392791033)

[8.0 PLAN ADMINISTRATION 15](#_Toc392791034)

[8.1 Plan Approval Procedures 15](#_Toc392791035)

[8.2 Plan Distribution Procedures 15](#_Toc392791036)

[8.3 Plan Maintenance Procedures 15](#_Toc392791037)

[9.0 SUPPORTING DOCUMENTATION 16](#_Toc392791038)

[END OF DISASTER RECOVERY PLAN 17](#_Toc392791039)

[Appendix A: Approvals 17](#_Toc392791040)

# DOCUMENT NOTES

**Disaster Recovery Plan Purpose:**

The purpose of this Disaster Recovery Plan is the high level documentation of disaster recovery related strategies, procedures, decisions and related practices.

**Document Control:**

Use this space to record notes and information regarding DRP preparation and version control. Add rows to the table to make additional entries.

|  |  |  |  |
| --- | --- | --- | --- |
| Entry # | Date | Version | Notes |
| 1 | Click here to enter a date. | 1.0 | The first draft of the Disaster Recovery Plan is created. |

# 1.0 STATEMENT OF GOALS AND OBJECTIVES

Use this space to present an overview of the purpose and content of your Disaster Recovery Plan. As this section is documented, the following questions should be considered:

What are your disaster recovery planning goals?

*Examples:*

* *To provide operational continuity and quick recovery for all critical systems impacted by a technology related disaster event.*
* *To ensure that the disaster recovery program is properly communicated to all staff, clearly identifying all essential roles and responsibilities.*
* *To ensure adherence to established safety procedures, exit plans and related emergency requirements.*
* *To maintain an orderly process for business resumption and systems recovery.*
* *To ensure that disaster recovery activities and strategies are continually tested and revised as needed.*

How will this plan be used and distributed within your organization?

How will this plan be integrated with other business recovery and employee safety plans?

Why is this plan important and valuable to your organization?

# 2.0 PLANNING ASSUMPTIONS

### 2.1 Requirements Assumptions

* State the plan “subjects” (identifying the systems and services to which this plan applies).
* State the business locations and operational units to which the plan applies.
* List the established disaster recovery “priorities”:
  + Identify critical business operations and functions.
  + Identify critical systems and related IT services.

### 2.2 Recovery Assumptions

* List the systems covered and the capacity to be restored, as in this example:
  + *50% of critical functions will be restored within 24 hours.*
  + *100% of critical functions will be restored within 48 hours.*
* List the scenario conditions covered by the plan. *(Examples: Business Site Down, Technology Site Down, All Sites Down, Technology Down)*
* Specify the outage duration addressed by the plan.  *(Example: This plan applies to disaster events lasting no longer than 60 days)*
* List the dependencies. *(Example: List the vendors, external support providers or internal support groups upon which the plan performance relies).*
* List the exclusions.  *(Identify any disaster conditions not covered by the plan. Example: “This plan is not designed to address disasters occurring in foreign locations”)*

# 3.0 PLAN ACTIVATION CRITERIA

As this section is documented, the following questions should be addressed:

## 3.1 Plan Activation Criteria

* What types of events will trigger plan activation?

## 3.2 Plan Activation Procedures

* How will these events be evaluated to ensure that plan activation is appropriate?
* Who will be involved in this event assessment process?
* How will assessment recommendations be escalated to the appropriate decision makers?
* Who must approve plan activation?
* How will the plan be activated?
* What are the activation approval requirements?
* How will plan activation be communicated?

# 4.0 SCENARIOS AND RESPONSE STRATEGIES

This section is used to identify the disaster scenarios covered by this plan, and the designated response strategy associated with each. Add rows as needed for additional scenarios.

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario  Description** | **Planned Response Strategy** | **Expected Response Results** | **Post-disaster Expectations** |
| Describe the scenario.  *Example: Temporary loss of access to main office site.* | Describe the planned response.  *Example: Activate the hot-site.* | Describe the expected response result.  *Example: 75% of all critical functions will be active at the hot-site in 4 hours.* | Describe expected post-disaster activities.  *Example: Once the main office is accessible, data entries created at the hot-site will be restored to production systems.* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 5.0 DISASTER RECOVERY REQUIREMENTS

## 5.1 Technology Requirements

* What types of critical systems are currently in place?
* How are these systems configured?
* Where are these systems located?
* What role do these systems play in business operations? (Issues to address: how are they used, by whom, and for what purpose?)
* Why have these systems been designated as critical and essential to business continuity?
* What types of hardware and software devices (including data) will be required to establish and maintain critical business operations in the event of a technology related disaster?

## 5.2 Operational Requirements

* How does your business/organization/department operate?
* What are the most critical business operations?
* What are the most critical job functions?
* How is technology used to support these critical business operations and job functions?
* What types of services does [the department] provide to the organization?
* What role do these services play in the disaster recovery and business resumption process?
* How will these services be maintained during a disaster condition?
* Will external or temporary resources be required to maintain technology related support services during a disaster condition?

## 5.3 Communications Requirements

* How will internal communication be ensured and maintained during, and after a disaster event?
* How will communications systems (telephones, wireless, email, internet, and intranet) be used to communicate during and after a disaster event?

## 5.4 Backup Requirements

* What types of backups will be required?
* What is the required backup schedule?
* Where will backups be stored?
* How much time is required to restore critical data?

## 5.5 Documentation Requirements

* What types of documents will be required to support the disaster recovery process?

## 5.6 Supplies Requirements

* What types of business equipment (non-computing) and office supplies will be needed to support the disaster recovery process?

## 5.7 Training Requirements

* What types of training will be provided to technology staff to support the disaster recovery process?
* What types of training will be provided to non-IT staff and employees to support the disaster recovery process?
* What types of training (and/or information) will be provided to external service providers and customers (if applicable) in support of the disaster recovery process?

# 6.0 DISASTER RECOVERY PROCEDURES

This section should be used to specify “step-by-step” procedures to be followed in the event of a covered disaster event:

## 6.1 Communications Procedures

* Emergency contact information for employees, customers, vendors and any other groups or individuals as needed for plan support (including primary and alternate contact designations).
* Communications Step-by-Step: detailing the “disaster-related” use and availability of telephones, wireless devices, voicemail, email, intranet and the company web site.
* Escalation procedures to be followed in the event of a declared disaster considering the recovery and response “chain of command” and the use of one or more Command Center locations.
* Steps and procedures to provide ongoing “how-to” information during the crisis event (to keep staff informed on current status, and day-to-day business procedures).

## 6.2 Remote Access Procedures

* What types of job functions and internal operations can be performed from a home office location?
* What type of hardware and software will be required?
* Will end-users require any special training?
* How will alternate systems and remote access procedures be activated and communicated to end-users?

## 6.3 Technical Implementation Procedures

* How will systems be installed, configured and administered during a covered disaster event (considering alternate work locations and alternate operating procedures)?

## 6.4 Backup and Data Recovery Procedures

* How will backups be retrieved in the event of disaster plan activation?
* How will data backups be restored for emergency and long term access?

## 6.5 Temporary Access Procedures

* How will access be provided to alternate hardware and software systems (considering user-ids, passwords, applications and data)?
* How will access be provided to any alternate office/business resumption sites?

## 6.6 Technical Support Procedures

* Who will be responsible for technical support during a covered disaster event?
* What types of technical support services will be provided?
* During what period of the day will support services be available?
* How will support requests be submitted, organized, resolved and closed during the disaster event?

## 6.7 Alternative Operating Procedures

* Which business operations can be met with the use of standalone computers?
* For how long can these standalone operations be used to serve temporary business needs?
* What steps must be taken by technology support staff and/or end-users to complete the transition to any standalone computing operations?
* How will critical data files be made available during the crisis period?
* Which business operations can be met with the use of manual operational procedures?
* For how long can these manual operations be used to serve temporary business needs?
* What tools will be required to maintain these manual operations (i.e. forms, information, policies and procedures)?
* What are the hardware and software requirements needed to support alternate operating procedures?

# 7.0 ROLES AND RESPONSIBILITIES

## 7.1 Disaster Recovery Team Mission Statement

Use this space to document your team mission statement:

* What is the purpose of your Disaster Recovery Team?
* What primary goals and objectives for team organization and structure?
* How will the team operate within the overall organizational structure?

## 7.2 Organizational Chart

The following chart illustrates managerial roles and reporting relationships for the Disaster Recovery Team.

**Sample Organizational Notes**:

* The **DRP Steering Committee** has management oversight and executive authority over the disaster recovery program.
* The **DRP Auditor** is responsible for disaster recovery planning verification and compliance.
* The **Disaster Recovery Coordinator** has day-to-day management authority over the execution and maintenance of the disaster recovery program.
* The **Planning Team** is responsible for all disaster recovery planning activities including data collection, requirements analysis, test planning, and end-user liaison activities.
* The **Technology Team** is responsible for the specification and design of all technology based disaster recovery solutions.
* The **Operations Team** is responsible for the implementation and execution of the disaster recovery plan, including test plans.
* The **Support Team** is responsible for any technical support and customer service tasks and activities needed to execute the disaster recovery program
* The **Administration** Team is responsible for all administrative aspects of maintaining and supporting the disaster recovery program.

## 7.3 Resource Requirements

* What types of resources and skills are required to properly plan and support disaster recovery activities?
* How many staff resources (in numbers and/or hours) are required to implement and maintain your disaster recovery program?
* How many additional staff resources (in numbers and/or hours) are required to manage and maintain systems in accordance with disaster recovery and business resumption requirements?
* What are the required DRP roles and responsibilities?
  + DRP Leadership
  + DRP Planning
  + DPP Technical Design
  + DRP Activation
  + DRP Support
  + DRP Compliance
  + DRP Verification
  + DRP Maintenance
* Who will fill these DRP roles and responsibilities?

# 8.0 PLAN ADMINISTRATION

When documenting this section, the following issues and questions should be considered:

## 8.1 Plan Approval Procedures

* How will the plan be approved?

## 8.2 Plan Distribution Procedures

* How will the plan be distributed?
* Who must receive the plan?

## 8.3 Plan Maintenance Procedures

* How will the plan be maintained and updated?
* How should questions and feedback be submitted?
* How will the plan be tested and verified?

# 9.0 SUPPORTING DOCUMENTATION

This section should be used to identify all related documents and information needed to support the plan and all related implementation procedures. (Note: Add rows to insert additional items).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Title** | **Date** | **Version** | **Location** | **Contact** |
| DRP Team Contact List | Click here to enter a date. | 1.0 | Attachment | Name/Title/email |
| Company Phone List | Click here to enter a date. | 1.0 | Attachment | Name/Title/email |
| Organization Chart | Click here to enter a date. | 1.0 | Attachment | Name/Title/email |
| End-User Support Procedures | Click here to enter a date. | 1.0 | Server/Folder /Filename | Name/Title/email |
| Service Level Agreement | Click here to enter a date. | 1.0 | Server/Folder /Filename | Name/Title/email |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# END OF DISASTER RECOVERY PLAN

## Appendix A: Approvals

Name: Who is approving this Disaster Recovery Plan?

Title: What is that person’s title?

Department: What is that person’s department?

Contact Phone: What is that person’s contact phone?

Contact Email: What is that person’s contact email?

Date: Click here to enter a date.