thrivenextgen.com

THRIVE℠

Disaster Recovery Plan

A template to inventory your organization’s IT infrastructure and critical information, and to develop a detailed plan to restore service and recover in the event of a disaster.

Table of Contents

Introduction

Hardware fails, hackers attack, data gets corrupted and disasters happen. Use this template to create your Disaster Recovery Plan to prepare your organization for common IT-based business disruptions and incident response.

Whether you are managing your DR Plan internally or are entrusting your plan to a managed service provider, the document must contain detailed, accurate and up-to-date information about the IT operations of your organization. The DR Plan must present that information in a clear and coherent format that is easily consumable and – most importantly – actionable during an actual emergency. What happens if the key personnel that are usually responsible for your DR Plan aren't available? Your employees or service provider must be able to follow the document and react rapidly so that systems' availability can be restored based on your established service level requirements.

DR Plans need to support the business's objectives. What is the impact on your business if your environment is not available for your customers to access? Do you need to recover the entire environment, or will a smaller percentage be enough for a short period of time? This template is meant as a guide only. You should review it carefully to determine whether it appropriately fits your needs. If desired, our services team can guide you through a process to customize the template or create a comprehensive DR Plan that best meets your own requirements and goals.

At a Glance

A Disaster Recovery Plan template (DR Plan) is a detailed IT document that provides a blueprint for recovering from common IT-based business disruptions like:

- **Environmental Catastrophes**
- **Building Accessibility or Power Disruption**
- **Ransomware or Other Cyberattacks**
- **Hardware Failures**
- **Software Failures**
- **Network Failures**
- **Data Corruption**
- **Employee Errors**

Step 1: Define What Constitutes a Disaster for Your Organization

Defining Your Disasters

A disaster can be caused by many events resulting in your IT department not being able to perform some or all of their regular roles and responsibilities for a period of time.

Your Organization defines disasters as meeting at least one of the following conditions:

□ **1. One or more vital systems are non-functional**

   a. Define the tiers of criticality; status examples include Critical, Medium, Low

   b. Establish Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each tier

   c. Assign a criticality status (and related RTO/RPO) to each application and system

   Example: Critical: Production server, <4 hrs RTO, backups every 1 hr RPO

□ **2. The building is not available for an extended period of time but all systems are functional within it**

□ **3. The building is available but all systems are non-functional**

□ **4. The building and all systems are non-functional (e.g. “smoking hole”)**

□ **5. Network connectivity is not available**

Notes:

Step 1: Define What Constitutes a Disaster for Your Organization

Activation Criteria

The following events can result in a disaster, requiring this DR Plan to be activated.

Edit this list to reflect how your organization is mitigating against the following situations:

- □ Environmental disaster (flooding, hurricane, fire, etc.)
- □ Hardware failure / server room issue
- □ Network failure
- □ Power outage
- □ Theft or Insider threat
- □ Malicious actors i.e., ransomware
- □ Physical security incident
- □ Human error
- □ IT human resource gap

Step 2: Identify and Create Your Disaster Recovery and Supporting Teams

Create your DR Team and list the roles and responsibilities in this section. Can include contractors and managed services.

Team/Lead	First Name	Title	Phone & Email	Notes
Disaster Management Team				
Disaster Recovery Lead				
DR Coordinator				
Network Team				
Network Lead				
Network Admin				
Server Team				
Server Lead				
Server Admin				
Applications Team				
Applications Lead				
Applications Admin				

If additional info is available elsewhere, detail where:

Notes:

Step 3: Authorized to Declare Disaster

A list of who is authorized to declare a disaster. Can include contractors and managed services.

First Name	Last Name	Title	Phone & Email	Notes

If additional info is available elsewhere, detail where:

Notes:

Step 4: Emergency Contacts

Internal Contacts

Prepare a list of internal stakeholders and their roles around preventing and recovering from a disaster.

Role/Issue	First Name	Last Name	Title	Phone & Email	Notes
Application failure					
Network failure					
Security breach					
Escalations & approvals					

If additional info is available elsewhere, detail where:

Notes:

Step 4: Emergency Contacts

External Contacts

List your external resources and their contact details ahead of an incident so your team can reach them in a crisis without delay.

Vendor Type	First Name	Last Name	Title	Phone & Email	Notes
Property Management					
Power Company					
Power Generator					
Security Company					
Network Provider					
Telecom Carrier					
Managed Services					
Off Site Storage					
Server Supplier					
Workstation Supplier					
Insurance					
3rd Parties that require access					

If additional info is available elsewhere, detail where:

Step 5: Restore IT Functionality

Should an incident actually occur and Your Organization needs to exercise this DR Plan, this section will be referred to frequently as it will contain all of the information that describes the way Your Organization 's information system will be recovered.

Some examples of this important information to include in this section are:

- □ all Standard Operating Procedures documents
- □ Run-books
- □ Network diagrams
- □ Software licensing information
- □ Software deployment information
- □ Other:

Where are these resources located?

Notes:

Step 6: Current System Architecture

Insert a detailed **system architecture** diagram that identifies **all of your systems** and their locations.

If additional info is available elsewhere, detail where:

Step 7: Current Network Architecture

Insert a detailed **network architecture** diagram that identifies **all of your devices** and their locations.

If additional info is available elsewhere, detail where:

Step 8: Assess IT Systems' Criticality and Restoration Priority

Please list all of the IT Systems in your organization in order of their criticality. Next, list each system's components that will need to be brought back online in the event of a disaster.

System Name	Priority Rank	Description	System Components	Owner/ Responsibility	Notes

If additional info is available elsewhere, detail where:

Step 9: Assess Software Licensing Required and Restoration Responsibilities

Please list all of the software and applications in your organization in order of their criticality. Next, rank them in order that will need to be brought back online in the event of a disaster.

Include information around whether their related settings and data are stored with the software provider, or are within your systems and realm of responsibility to backup and restore.

1. **[Name of Software #1] Rank:** ______________________________

    License Number: ______________________________

    License Provider: ______________________________

    Data Backup and Restoration Status: ______________________________

2. **[Name of Software #2] Rank:** ______________________________

    License Number: ______________________________

    License Provider: ______________________________

    Data Backup and Restoration Status: ______________________________

3. **[Name of Software #3] Rank:** ______________________________

    License Number: ______________________________

    License Provider: ______________________________

    Data Backup and Restoration Status: ______________________________

Repeat as needed.

Step 10: Assess Network Locations and Connectivity

Locations

Please list all of the locations where your systems operate and where data is stored, along with key information about each.

1. **[Name of Site Location #1]** ______________________________

   Address: ______________________________

   Provider / Carrier: ______________________________

   Circuit Type: ______________________________

   Bandwidth: ______________________________

   CPE Gear required: ______________________________

   Model: ______________________________

2. **[Name of Site Location #2]** ______________________________

   Address: ______________________________

   Provider / Carrier: ______________________________

   Circuit Type: ______________________________

   Bandwidth: ______________________________

   CPE Gear required: ______________________________

   Model: ______________________________

Repeat for each site.

Step 11: Assess Network Equipment and Hardware

Network Equipment

Please list all of the locations and their network devices, along with key configuration and hardware information about each.

[Name of Site Location #1] ______________________________

Switches (make/model): ______________________________

Routers (make/model): ______________________________

Load Balancer (make/model): ______________________________

VPN Devices (make/model): ______________________________

Firewalls (make/model): ______________________________

Misc Network Appliances (make/model): ______________________________

Co-Location Equipment

[Name of Site Location #1] ______________________________

Servers: ______________________________

Storage devices: ______________________________

Telecom/Voice equipment: ______________________________

Repeat for each site.

Step 12: Plan Testing and Maintenance

While efforts will be made to construct this DR Plan in as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. DR testing is an iterative process. Additionally, over time the Disaster Recovery needs of the organization will change. There is a need to re-sync the DR Plan with the business needs on an ongoing basis. As a result of these two factors this plan will need to be tested. You should establish the level of testing in your DR Plan and the specific activities should be documented. Two phases of testing are as follows:

DR Rehearsal

Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses ("table top exercises"). This test provides the opportunity to review a plan with a larger subset of people, allowing the DR Plan Lead to make appropriate changes to the plan. Staff will also become familiar with procedures and equipment.

Failover Testing

Under this scenario, servers and applications are brought online in an isolated environment. There is no impact to existing operations or uptime. Systems administrators or MSP partners ensure that all operating systems come up cleanly. Application administrators validate that all applications perform as expected. Typically testing is done as sub-set testing with a sampling approach. One can have multiple sub-set tests to validate the overall DR readiness.

Step 12: Plan Testing and Maintenance

Live-Failover Testing

A live-failover test activates the total DR Plan. The test will disrupt normal operations, and therefore should be approached with caution. Many organizations limit this test to control downtime. Ensure you have completed several iterations of rehearsal and failover testing (Phase 1 and 2) before proceeding with this step. Additionally, communicate all expected disruptions well in advance of performing this test.

Any gaps in the DR Plan that are discovered during the earlier phases will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require. Lessons learned from DR testing are crucial to the improvement of the DR Plan. Change control and incorporating it into the DR Plan also plays a huge factor in the success of DR testing.

Date of Last Live-Failover Testing: ____

Date of Next Scheduled Live-Failover Testing: ____________________________________

Notes:

THRIVE℠

thrivenextgen.com / 866-205-2810