**COMPANY**

Disaster Recovery Plan (DRP) for [ ]

## Table of Contents

[Table of Contents 1](#_Toc14338542)

[Things to Consider when editing this plan for your Company 2](#_Toc14338543)

[**1. Purpose and Objective** 3](#_Toc14338544)

[Purpose 3](#_Toc14338545)

[Scope 3](#_Toc14338546)

[**2. Business Impact Types** 4](#_Toc14338547)

[**3. Disaster Recovery Strategies** 5](#_Toc14338548)

[Explanation of scenarios 5](#_Toc14338549)

[**4. Disaster Recovery Procedures** 6](#_Toc14338550)

[Response Phase 7](#_Toc14338551)

[Failover Phase 8](#_Toc14338552)

[Data Center/Internal Resource Disruption Recovery 8](#_Toc14338553)

[Significant External Dependency Disruption Recovery 10](#_Toc14338554)

[Significant Network Disruption Recovery 11](#_Toc14338555)

[Resolution Phase 12](#_Toc14338556)

[Original Restoration Phase 13](#_Toc14338557)

[Data Center/Internal Resource Disruption Restoration 13](#_Toc14338558)

[Internal or External Dependency Restoration 13](#_Toc14338559)

[Significant Network Disruption Restoration 14](#_Toc14338560)

[**5. Maintenance of Plan** 14](#_Toc14338561)

[Appendix A: Disaster Recovery Contacts - Admin Contact List 15](#_Toc14338562)

[Appendix B: Document Maintenance Responsibilities and Revision History 15](#_Toc14338563)

[Appendix C: Glossary/Terms 16](#_Toc14338564)

To download the editable version of this document go to: <https://www.digitalindustry.com/free-guides/>

### Things to Consider when editing this plan for your Company

This document is a generic template compiled from various online sources such as Microsoft and internal experiences at Digital Industry. The entirety of the document needs to be reviewed and edited to fit the intended purpose.

Special Note:

All language highlighted Should be replaced with details pertaining to your company

All sections highlighted Should be removed when finalizing document

#### Determine Scope and Size

* Agree upon level of scope
* Can a “non-IT shop” person come in and understand the plan?
* Is the plan practical?
* Do we outsource the plan?

#### Definitions of Disaster

A.What are (and what are *not*) the criteria to determine a disaster?

* Physical, data, hardware, user interface, ext.
* How do we know if a disaster has been detected?
* What kinds of redundancy do you have in place on your systems & services?

#### Examples of Disaster Criteria

* Outage by hours
* Outage by hours greater than certain level requiring contact of disaster team to declare disaster
* When day-to-day plans no longer work (i.e., day-to-day work drill is gone, or when there is a build-up, escalation procedures are exhausted, and operation no longer meets common baseline planning
* When there are threats that scope up to become a disaster
* When we lose a data center or building that houses the data center
* When we lose a core business service (i.e., email)
* When we require risk management and insurance to declare a disaster in order to get vendor action in recovery

It is important that every company develops its own definitions of disaster that are practical as opposed to just the industry standard definitions.

# Purpose and Objective

### Purpose

COMPANY developed this disaster recovery plan (DRP) to be used in the event of a significant disruption to business systems. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

### Scope

The scope of this DRP document addresses technical recovery in the event of a significant disruption. The intent of the DRP is to be used in conjunction with a Business Continuity Plan (BCP). A DRP is a subset of the overall recovery process contained in the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies not directly relevant to the technical recovery outlined herein are included in the Business Continuity Plan and/or the Corporate Incident Response and Incident Management Plan.

This disaster recovery plan provides:

1. Insight about different **types of technical business impact**
2. Technical **response flows** and recovery strategies
3. Guidelines for **recovery procedures**
4. References to key **Failover Plans** and technical dependencies
5. **Rollback procedures** that will be implemented to return to [standard operating state](#Standard_Operating_State)
6. **Contacts** for key internal/external resources
7. Guidelines on keeping this document up to date

The specific objectives of this disaster recovery plan are to:

* Immediately mobilize a core group of leaders to assess the technical ramifications of a situation
* Set technical priorities for the recovery team during the recovery period
* Minimize the impact of the disruption to the impacted features and business groups
* Stage the restoration of operations
* Enable rollback operations once the disruption has been resolved if determined appropriate by the recovery team

This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

# Business Impact Types

This section outlines the types of business impacting disasters identified during the development of this disaster recovery plan. This may vary from company to company depending on types of services & systems in use.

|  |  |  |
| --- | --- | --- |
| Business Impact Types | Assumptions | Examples |
| Presentation Layer  Presentation components | * Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g. client or server side, web interface or downloaded application). * Infrastructure and back-end services are still assumed to be active/running. | * Outlook email issues * Web portal not functioning properly |
| Business Intelligence / Reporting  Processing  Layer | * The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted). * Standard backup processes (e.g. tape backups) are not impacted, but the active / passive or mirrored processes are not functioning. * Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing. | * Phone system call logs not working * Core application data trail not functioning |
| Network Layers  Infrastructure components | * Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers. * Assumption is that terminal connections, serially attached devices and inputs are still functional. | * Access to internet is down * Internet is very slow latency |
| Database Layer  Database/File storage components | * Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable | * Issue accessing files * Corruption or virus * Lock files |
| Hardware/Host Layer  Hardware components | * Physical components are unavailable or affected by a given event | * Major hardware failure * Fire/Flood in office |
| Virtualizations (VM's)  Virtual Layer | * Virtual components are unavailable * Hardware and hosting services are accessible | * Unable to access Virtualized services/resources |
| Administration  Infrastructure Layer | * Support functions are disabled such as management services, backup services, and log transfer functions. * Other services are presumed functional | * Management portals inaccessible |
| Internal/External  Dependencies | * Interfaces and intersystem communications corrupt or compromised | * Data flow to database from applications is not working * ISP is down |

*In addition, assumptions within the Business Continuity Plan for this work stream still apply.*

# [Disaster Recovery Strategies](#Disaster_Recovery_Strategy)

The overall DR strategy of COMPANY is summarized in the table below and documented in more detail in the supporting sections. These scenarios and strategies are consistent across the technical layers (user interface, reporting, etc.)

### Explanation of scenarios

**Data Center/ Internal resource disruption**: refers to inability to utilize resources located in a network closet or a data center. In this scenario the hardware & resource are owned by the company.

**Significant External Dependency Disruption:** Refers to a disaster due to the inability to utilize a resource not owned by the company, but is a dependency, like cloud phones services or cloud exchange.

**Significant Network Disruption**: Refers to a disaster due to a network outage. Could be due to hardware failures, issues due to changes, or due to external provider.

**Things to consider when defining scenarios and strategies:**

These Strategies will change on a company to company Basis, depending on factors like:

* Location of critical services
  + Cloud
  + On Premise
* Criticality of services
* Capabilities of hardware/services
* Availability of redundancy + resources

For example, if your company does not have a data center, that section may not apply

# Disaster Recovery Procedures

A disaster recovery event can be broken out into four phases, the response, the failover, the resolution, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan.

*Each of these phases are broken down on the following pages*

### Response Phase

The following are the activities, parties and items necessary for a DR response. Please note these procedures are the same regardless of the triggering event (e.g. whether caused by a Data Center disruption or other scenario).

#### Response Phase Recovery Procedures – All DR Event Scenarios

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Identify issue, Inform relevant parties / Designated Responsible Individual (DR Manager) | OPS Manager | \_\_ minutes | * Issue communicated / escalated * Priority set |
| Identify the team members needed for recovery / resolution (DR Team) | DR Manager | \_\_ minutes | Selection of core team members required for restoration phase from among the following groups:   * Operations/ Technical |
| Establish a conference line for a bridge call to coordinate next steps | DR Manager | \_\_ minutes | Primary bridge line: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Secondary bridge line: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  Alternate / backup communication tools: email, communicator |
| Communicate the specific recovery roles and determine which recovery strategy will be pursued. | DR Manager | \_\_ minutes | * Documentation / tracking of timelines and next decisions * Determine recovery Strategy * Creation of disaster recovery event command center / “war room” as needed |

This information is also summarized by feature in [Appendix A: Disaster Recovery Contacts - Admin Contact List](#_Appendix_A:_Disaster).

### Failover **Phase**

During the failover phase, the steps taken to enable recovery will vary based on the type of issue. Samples for the procedures for each recovery scenario are listed below.

### Data Center/Internal Resource Disruption Recovery

#### Failover All Services to Alternate Source

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Initiate Failover | DR TEAM | TBD | * Restoration procedures identified * Risks assessed for each procedure * Coordination points between groups defined * Issue communication process and triage efforts established |
| Complete Failover | DR TEAM | TBD | * Recovery steps executed, including handoffs between key dependencies |
| Test Recovery | DR TEAM | TBD | * Tests assigned and performed * Results summarized and communicated to group |
| Failover deemed successful | DR TEAM | TBD | * Move to phase 3 |

#### Reroute Core Processes to Alternate Source

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### Operate at Deprecated Service Level

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### Take No Action – monitor for resource recovery

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the Data Center is fully in the control of another department or vendor).

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Track communication and status with the core recovery team. | DR TEAM | As needed |  |
| Send out frequent updates to core stakeholders with the status. | DR TEAM | As needed |  |

Insert a timeline for recovery actions associated with the failover the technical components between different data centers to provide geo-redundant operations. Coordination of recovery actions is crucial. A timeline is necessary in order to manage recovery between different groups and layers.

Incident + 15min – AAAA

Incident + 30min – BBBB

Etc…

[ Insert timeline for Recovery here ]

### Significant External Dependency Disruption Recovery

#### Reroute operations to backup provider

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### Participate in Recovery Strategies Collaboratively with the Vendor

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Inform other teams about technical dependencies | DR TEAM | As needed |  |
|  | DR TEAM | As needed |  |

#### Take No Action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the disruption is fully in the control of another department or vendor).

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Track communication and status with the core recovery team. | DR TEAM | As needed | * Provide feedback about SharePoint service availability |
| Send out frequent updates to core stakeholders with the status. | DR TEAM | As needed |  |

### Significant Network Disruption Recovery

#### Reroute Operations to Backup Provider

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
|  |  |  |  |
|  |  |  |  |

#### Execute available recovery procedures

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Inform other teams about technical dependencies | DR TEAM | As needed | * Hardware (CPU, Memory, Hard disk, Network requirements) |
| Teams | DR TEAM | As needed |  |
|  | DR TEAM | As needed |  |

#### Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the internal or external dependency is fully in the control of another department or vendor).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Step | Owner | Duration | | Components | | |
| Track communication and status with the core recovery team. | | | DR TEAM | | As needed | * Provide feedback about SharePoint service availability | |
| Send out frequent updates to core stakeholders with the status. | | | DR TEAM | | As needed |  | |

### Resolution Phase

During the resolution phase: The steps taken to restore the services will vary based on what service it is and what the issue going on is. The general steps are listed below, that apply in most scenarios

This phase can be done alongside or after phase #2 but must be completed before proceeding to phase #4

#### Resolution Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Troubleshoot & Isolate Issue | DR TEAM | TBD | * Issue is Identified |
| Resolution plan put together | DR TEAM | TBD | * Plan for resolving including what resources are required to complete * Plan to test * Plan communicated with all involved parties |
| Plan is executed | DR TEAM | TBD | * Services issues are resolved & tested * DR team can proved with restoration * Resolution is communicated to all parties included |
| Evaluation of disaster | DR TEAM  & DR Manager | TBD | * Review disaster and discuss ways to avoid having issue reoccur |

## Original Restoration Phase

During the restoration phase, the steps taken to restore services will vary based on the type of issue. The general steps are listed below, that apply in most scenarios.

### Data Center/Internal Resource Disruption Restoration

#### Full-Service Restoration

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Determine whether failback to original Data Center will be pursued | DR TEAM | TBD | * Restoration procedures determined |
| Complete Failback | DR Team | TBD | * Failback steps executed, including handoffs between key dependencies |
| Test Failback | DR Team | TBD | * Tests assigned and performed * Results summarized and communicated to group * Issues (if any) communicated to group |
| Determine whether failback was successful | DR TEAM | TBD | * Declaration of successful failback and communication to stakeholder group. * Disaster recovery procedures closed. * Results summarized, and DRP updated (as needed). |

The following section contains steps for the restoration procedures.

### Internal or External Dependency Restoration

#### Execute available recovery procedures

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
|  | DR TEAM | As needed |  |
|  | DR TEAM | As needed |  |

#### Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the disruption is fully in the control of another department or vendor).

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Track communication and status with the core recovery team. | DR TEAM | As needed | * Provide feedback about SharePoint service availability |
| Send out frequent updates to core stakeholders with the status. | DR TEAM | As needed |  |

### Significant Network Disruption Restoration

#### Execute available recovery procedures

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
|  | DR TEAM | As needed |  |

#### Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the internal or external dependency is fully in the control of another department or vendor).

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Owner | Duration | Components |
| Track communication and status with the core recovery team. | DR TEAM | As needed |  |
| Send out frequent updates to core stakeholders with the status. | DR TEAM | As needed |  |

# Maintenance of Plan

1. Documentation repository
2. Plan must be maintained annually, BUT parts of the plan need to be updated more frequently (for ex., phone lists)

* Plan should be in a dynamic database that can be updated automatically

1. “Who does what” for DR plan maintenance?

* Who updates what section?
* Prints copies of the plan?
* Who files the plan?
* Kept with which members at home or in trunk of car?
* Kept on wallet card? (DRP team instructions)
* Who keeps log for audit of the maintenance?

1. Changes to the asset inventory should automatically update the disaster recovery plan
2. Problems with testing the plan should cause an update of plan
3. Return to Day-to-Day Operations

* Have maintenance agreements in place
* Have customer service level agreements in place (sign-offs)

## Appendix A: Disaster Recovery Contacts - Admin Contact List

The **critical team members** who would be involved in recovery procedures for feature sets are summarized below.

|  |  |
| --- | --- |
| Internal Position Name | Contact Info |
| DR Manager – John Doe | 123-456-7890 / jdoe@email.com |
|  |  |
|  |  |
|  |  |
|  |  |

For the key external dependencies identified, the following are the primary contacts.

|  |  |  |  |
| --- | --- | --- | --- |
| Dependency | Company | Name | Contact Information |
| Internet Services | Verizon | John Doe | 123-456-7890 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Appendix B: Document Maintenance Responsibilities and Revision History

This section identifies the individuals and their roles and responsibilities for maintaining this Disaster Recovery Plan.

**Primary Disaster Recovery Plan document owner is:**

Primary Designee:

Alternate Designee:

#### Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of Person Updating Document | Date | Update Description | Version # | Approved By |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Appendix C: Glossary/Terms

**Standard Operating State**: Production state where services are functioning at standard state levels. In contrast to recovery state operating levels, this can support business functions at minimum but deprecated levels.

**Presentation Layer:** Layer which users interact with. This typically encompasses systems that support the UI, manage rendering, and captures user interactions. User responses are parsed, and system requests are passed for processing and data retrieval to the appropriate layer.

**Processing Layer:** System layer which processes and synthesizes user input, data output, and transactional operations within an application stack. Typically, this layer processes data from the other layers. Typically, these services are folded into the presentation and database layer, however for intensive applications; this is usually broken out into its own layer.

**Database Layer**: The database layer is where data typically resides in an application stack. Typically, data is stored in a relational database such as SQL Server, Microsoft Access, or Oracle, but it can be stored as XML, raw data, or tables. This layer typically is optimized for data querying, processing and retrieval.

**Network Layer**: The network layer is responsible for directing and managing traffic between physical hosts. It is typically an infrastructure layer and is usually outside the purview of most business units. This layer usually supports load balancing, geo-redundancy, and clustering.

**Hardware/Host Layer**: This layer refers to the physical machines that all other layers are reliant upon. Depending on the organization, management of the physical layer can be performed by the stack owner or the purview of an infrastructure support group.

**Virtualization Layer**: In some environments virtual machines (VM's) are used to partition/encapsulate a machine's resources to behave as separate distinct hosts. The virtualization layer refers to these virtual machines.

**Administrative Layer:** The administrative layer encompasses the supporting technology components which provide access, administration, backups, and monitoring of the other layers.