**Table of Contents**

[1. Introduction 3](#_Toc67584688)

[2. Useful Contacts 3](#_Toc67584689)

[2.1 Disaster Recovery Management Team 3](#_Toc67584690)

[2.2 3rd Party Contacts 3](#_Toc67584691)

[3. Disaster Recovery Plan 4](#_Toc67584692)

[3.1 Initiating a Disaster Recovery Plan 4](#_Toc67584693)

[3.2 Disaster Recovery Steps 4](#_Toc67584694)

[4. Disaster Recovery Risks 6](#_Toc67584695)

[5. Disaster Recovery Issues 6](#_Toc67584696)

**Document Control**

**Document Version History**

This table shows a record of significant changes to the document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description of Change** |
| 1.0 | 20/09/2020 |  | Initial Draft |
|  |  |  |  |
|  |  |  |  |

**Approvals**

This table shows the approvals on this document for circulation, use and withdrawal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Approver** | **Title/Authority** | **Approval Remarks** |
| 1.0 | 20/09/2020 | Swapnil Wale |  | Initial Draft |
|  |  |  |  |  |
|  |  |  |  |  |

**Document Distribution List**

|  |  |
| --- | --- |
| **Document User** | **Job Title** |
|  |  |
|  |  |
|  |  |

# Introduction

The DR (Disaster Recovery) Plan is a step-by-step manual on how to execute the plan in case a disaster occurs, and the DR Plan needs to be initiated. It also includes the related risks, issues, stakeholders and responsibilities for a successful execution of the plan.

# Useful Contacts

## Disaster Recovery Management Team

| **#** | **Name (First, Last)** | **DR Role** | **Contact Info** |
| --- | --- | --- | --- |
| 1 | Doris Calsolaro | DR Team Lead | (T[[1]](#footnote-1)) +818-247-1132  (M[[2]](#footnote-2)) +47-0879-6621  E-mail: Dcalso@example.com |
| 2 | Vishwas Devasia | DR Plan Architect | (T) +818-2224-8917  (M) +47-617-2030  E-mail: Vdev@example.com |
| 3 | Tom O’Leary | DR Communications Lead | (T) +242-200-3077  (M) +52-337-5681  E-mail: Tole@example.com |
| 4 | Nancy Ring-Day | DR PMO | (T) +335-057-6178  (M) +48-001-7093  E-mail: Nringd@example.com |
| 5 | Sharona Dinvits | DR Technician | (T) +818-090-3271  (M) +55-371-8317  E-mail: Sdin@example.com |

## 3rd Party Contacts

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Name (First, Last)** | **DR Role** | **Company Name** | **Contact Info** |
| 1 | Srinivas Panta | DR machine technician | VDR | (T) +974-3-277-6454  (M) +974-2733-1147  E-mail: Span@VDR.com |
| 2 | Fouad Ahamed | DR Electrician | VDR | (T) +974-3-270-6646  (M) +974-2733-7093  E-mail: Faha@VDR.com |
| 3 | Christine Lahey | DR Full Stack Expert | VDR | (T) +1-828-3756  (M) +1-2847-332  E-mail: Clah@VDR.com |

# Disaster Recovery Plan

## Initiating a Disaster Recovery Plan

The DR team will initiate a DR plan if any of the following circumstances are met

| **#** | **Priority** | **Owner** | **Circumstances** |
| --- | --- | --- | --- |
| 1 | P1 | DR Team Lead | The organizations’ servers are inaccessible for over 5 minutes by the users (no ping or remote access) |
| 2 | P1 | DR Team Lead | Over 75% of the users are affected by a disaster |
| 3 | P1 | DR Team Lead | The organizations’ website is down for over 5 minutes |
| 4 | P2 | DR PMO | The monitoring systems are down for over 30 minutes |
| 5 | P2 | DR Technician | The temperature of the primary server room is over 15° C |

## Disaster Recovery Steps

In case one of the circumstances in the table above (“Initiating a DR Plan”) is met, then the DR management team will initiate the DR Plan, and follow the steps detailed in the table below –

| **#** | **Step** | **Owner** | **Frequency** |
| --- | --- | --- | --- |
| 1 | Release a communication (E-mail and SMS) to all the stakeholders of the Project | DR Communications Lead | One Time |
| 2 | Analyze the current situation and find out what happened | DR Team Lead | One Time |
| 3 | Gather all the DR measurements, perform an analysis and issue a report | DR PMO | Once every 30 minutes for the first 4 hours, then once every 2 hours until resolution |
| 4 | Initiate the cutover procedure which includes - | DR Plan Architect |  |
| 4.1 | Switching the DR severs on |  | One Time |
| 4.2 | Diverting all the internet traffic to the DR data centre |  | One Time |
| 4.3 | Enabling the DR ports for the internal users |  | One Time |
| 4.4 | Running a diagnostic check that the RPO and RTO SLA’s were achieved |  | One Time |
| 4.5 | Take corrective actions |  | Every 30 minutes until step #4 is achieved |
| 4.6 | Check that the internal users can access the back-end server |  | One Time |
| 4.7 | Check that the internal users can access the front-end server |  | Every 30 minutes |
| 4.8 | Check that the external users can access the website |  | Every 30 minutes |
| 4.9 | Issue a press-release with clear explanations of the DR trigger, loss of information and next steps |  | Every 24 hours |
| 4.10 | Monitor the DR servers, data base and routers to make sure they’re not over-loaded |  | Every 90 minutes |
| 4.11 | Run a diagnostic check of the Primary data centre, and understand its current situation |  | Every 90 minutes |
| 4.12 | Formulate a plan on how to return to the primary data centre |  | One Time |
| 4.13 | Measure the primary data centres’ metrics to see if it’s possible to return to it |  | Every 120 minutes |
| 4.14 | Issue a press release with the plan on returning to the primary data centre |  | Every 24 hours |
| 4.15 | Execute the plan |  | On-Going |
| 4.16 | Measure the primary data centre’s metrics to make sure that the switch over is possible |  | Every 120 minutes |
| 4.17 | Understand why the switchover was necessary |  | One Time |
| 4.18 | Create a “lessons learned” document |  | One Time |
| 4.19 | Implement the document into the DR plan |  | One Time |
| 5 | Switch back top the primary data centre | DR Plan Architect | One Time |
| 6 | Update the DR plan document with the lessons learned | DR PMO | One Time |
| 7 | Update the risks table in the DR plan | DR PMO | One Time |
| 8 | Update the issues table in the DR plan | DR PMO | One Time |

# Disaster Recovery Risks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Risk** | **Probability[[3]](#footnote-3)** | **Impact[[4]](#footnote-4)** | **Mitigation** |
| 1 | The servers won’t be able to be switched on remotely | 20% | 5 | Have the 3rd party engineers on standby to manually turn the servers on |
| 2 | The traffic won’t be remotely routed to the DR data centre | 40% | 4 | Have the 3rd party engineers on standby to manually re-route the traffic to the DR data centre |
| 3 | There will be a loss of customers billing data for the last 3 minutes of transactions prior to the disaster | 60% | 3 | Offer the customers affected by this a 25% discount on their next purchase |

# Disaster Recovery Issues

| **#** | **Issue** | **Owner** | **Next Steps** |
| --- | --- | --- | --- |
| 1 | The backup generator in the DR data centre had only a 1/3 tank full | DR machine technician | 1. Check every week that the tank is full 2. Have an extra 100-gallon fuel barrel |
| 2 | The remote control of the DR stack wasn’t always possible | DR Full Stack Expert | 1. Insert an Out-Of-Band (OOB) remote control system in the DR servers 2. Test the OOB in the next DR drill |

1. Desk Telephone Number [↑](#footnote-ref-1)
2. Mobile Telephone Number [↑](#footnote-ref-2)
3. Probability of accruing, in increments of 20% [↑](#footnote-ref-3)
4. Impact in case the risk will come to fruition, in increments of 1 (1 to 5) [↑](#footnote-ref-4)