|  |
| --- |
| CrowSoft Technologies |
| Disaster Recovery Document |
|  |
| **Michael Mcfadden** |
| **Last reviewed & tested - 26/04/2019** |

# Introduction

This document covers the process and disaster recovery procedures in place at CrowSoft Technologies in case of a disaster. The disaster can be a geographical disaster or any other failure that leads to the Production Environment’s downtime. The purpose of this document is to ensure minimal downtime, data integrity and availability, in case of a disaster. This document will try to cover all the aspects that should be taken care in case of a disaster, as well as the safety of people. This document outlines the process and procedures that will help us overcome the disaster with minimal effect on the working of our organization

# Personnel

**Stake Holders & Responsibilities during a Disaster Recovery**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Job role** | **Contact details** | **DR process owned** |
| *Ruth Lennon* | *Product Owner* | *(Phone numbers, email address, normal workplace)* | *Oversees all decisions made as part of DR* |
| *Colin Kenny* | *IT sys admin* | *(Phone numbers, email address, normal workplace)* | *Backup and restore Jenkins pipeline and Git Repositories* |
| *Charles Aylward* | *IT sys admin* | *Phone numbers, email address, normal workplace)* | *Facilitate in coordination of recovery plan* |
| *Matthew McColgan* | *IT sys admin* | *Phone numbers, email address, normal workplace)* | *Backup and restore application code and database* |
| *Mary Walsh McGinty* | *IT sys admin* | *Phone numbers, email address, normal workplace)* | *Backup and restore server snapshots from VM* |
| *Liam Whoriskey* | *IT sys admin* | *Phone numbers, email address, normal workplace)* | *Backup and restore Documentation* |
| *Bharathi* | *IT sys admin* | *Phone numbers, email address, normal workplace)* | *Backup and restore Jenkins pipeline and Git Repositories* |
| *Joji* | *IT sys admin* | *Phone numbers, email address, normal workplace)* | *Backup and restore application code and database* |
| Michael McFadden | *IT sys admin* | *Phone numbers, email address, normal workplace)* | *Facilitate in coordination of recovery plan* |

# This DR Policy

## The major goals of this policy are as follows:

* 1. Ensure Personnel safety is number 1 priority
  2. To minimize interruptions to the normal operations.
  3. To limit the extent of disruption and damage.
  4. To minimize the economic impact of the interruption.
  5. To establish alternative means of operation in advance.
  6. To train personnel with emergency procedures.
  7. To provide for smooth and rapid restoration of service.

## Discovery - Policy Initiation

* 1. Notify Stakeholders
  2. Contact and set up disaster recovery team
  3. Set a disaster recovery team primary point of contact and incident center of command
  4. Determine degree of disaster
  5. Determine response first steps
  6. Determine estimated time to recovery complete
  7. Update senior management on initial findings
  8. Select appropriate disaster recovery procedure based on degree of disaster

## Response - Policy Response

* 1. Notify users of the disruption of service
  2. Implement proper application recovery procedure dependent on extent of disaster
  3. Monitor progress on recovery policy implementation through DR recovery team primary point of contact
  4. Contact backup site and establish a point of contact at that location
  5. Contact all other necessary personnel–both user and data processing–required for success of the recovery policy
  6. Contact vendors–both hardware and software–related to the disasters affected equipment

## Recovery - Recover from disaster

* 1. Determine applications to be run and in what sequence
  2. Ensure that all personnel involved know their tasks
  3. Make sure that the DR team at the disaster site has the necessary information to begin restoring
  4. Recover affected equipment from disk or tape media
  5. Verify recovered equipment is functioning properly
  6. Begin normal operations and notify staff of completion of recovery
  7. Review disaster process and document good/bad sections of the procedure

# Backups

* Server Snapshots – can be restored via recent snapshots
* Code Backups – Back up on Git repository
* Jenkins Pipelines Backups – Scheduled backups stored on server
* Database backups – Adhoc backups saved locally
* Documentation Backups – Adhoc backup saved to shared one drive

Backups should be accessible in a timely manner in order to restore them to your recovery servers. The best solution is to store your data backups in multiple offsite locations. Another solution is to store backups or data on a cloud platform that guarantees the five 9’s, 99.999% availability. Due to the restriction of the college project, the above backup policies would be carried out as best practice.

Restore Procedures

* Manual Restore from backups if we lose a server or source code
* Rebuild from scratch - Refer to Flipping book Binder link below for all set up procedures

# Supporting Documemtation

* Flipping book Binder: <https://online.flippingbook.com/view/22284/14/>
* OneDrive videos: <https://studentlyit-my.sharepoint.com/personal/l00113360_student_lyit_ie/_layouts/15/onedrive.aspx>
* Videos: <https://www.youtube.com/playlist?list=PLQYTpRHapl6FHiupp7bP0LyOQzR1bf8L2>

# Risk Management

Risk management involves the identification of risks and their causes;

Risk factors can be categorized as (Gupta 2008):

 Technical

 Environmental

 Managerial

 Organisational

Balancing disaster recovery planning with risk management will save money in the long run while offering adequate protection from the most likely disasters. Ideally, a disaster recovery plan will protect your company from every foreseeable disaster and return your company to full operations in the shortest possible amount of time. Unfortunately, this is cost prohibitive. You simply cannot afford to protect your organization against every possible disaster. Selecting which scenarios and how to protect your company against them is called risk management.

## **Disaster risk management approach**

## Risk prevention

Risk analyses to identify the hazards and how exposed the business is and can reveal what can be done to prevent or minimize damage, steps can then be taken to strengthen the defences

## Addressing residual risk

Even when prevention measures are put in place, every scenario can’t be accounted for due to often the cost and effort to cover every scenario. .Ex-ante financing such as specific insurance policies to certain disasters, which may be too costly to attempt to prevent ,can be obtained to help finance such a recovery plan .Ex-post financing will severely affect the business as all costs will have to be met by the company

## Preparing

Prepare for a disaster by ensuring a disaster recovery plan is put in place, this plan if well thought out and tested will ensure a speedy and cost-efficient recovery.

## Responding

Following a disaster, a quick response will ensure further damage to the business and lower the cost of recovery. The DRD will come into play here again with everyone knowing their roles and the Ex-ante financing that was put in place will aid and make the recovery more successful.

## Recovery

The recovery process can now begin with the help of the ex-ante financing to aid the recovery and lessons learnt from the disaster can be used as opportunities to improve the rebuilding of the business. These will help in preventing the same disaster from occurring again.