Disaster Recovery Plan
Version 9

REZOLVE.ai

Document Information

Nameof the document	DR Plan
Release date	19-Dec-2018
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Reviewed and no change
4	02-Dec-2021	Updated - Key Personnel Contact Info, Notification CallingTree, External Contacts, External Contacts Calling Tree, Risk Management, Emergency Alert
5	04-Mar-2022	Updated Document Information
6	01-Mar-2023	Updated - Key Personnel Contact Info, Notification CallingTree, External Contacts, External Contacts Calling Tree, Risk Management, Emergency Alert
7	23-Sep-2024	Updated - Key Personnel Contact Info, Notification CallingTree, External Contacts, External Contacts Calling Tree, Risk Management, Emergency Alert
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Updated Key personal contacts infor, Notification calling tree, external contacts

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	04-June-2026

Table of Contents

1 Information Technology Statement of Intent 3
2 Our Mission 3
3 Policy Statement 3
4 Objectives 3
5 Key Personnel Contact Information 3
6 Notification Calling Tree 4
7 External Contacts 4
8 External Contacts Calling Tree 6
9 Plan Overview 6
10 Plan Updating 6
11 Plan Documentation Storage 6
12 Backup Strategy 6
13 Risk Management 7
14 Emergency Response 7
15 Alert, Escalation and Plan Invocation 7
16 Plan Triggering Events 7

17 Assembly Points 7
18 Activation of Emergency Response Team 8
19 Disaster Recovery Team 8
20 Emergency Alert, Escalation and DRP Activation 8
21 DR Procedures for Management 9
22 Contact with Employees 9
23 Alternate Recovery Facilities / Hot Site 9
24 Personnel and Family Notification 9
25 Media 9
26 Media Contact 9
27 Media Strategies 9
28 Media Team 9
29 Rules for Dealing with Media 9
30 Insurance 10
31 Financial and Legal Issues 10
32 Financial Assessment 10
33 Financial Requirements 10
34 Legal Actions 10
35 DRP Exercising 10
36 Appendix A – Suggested Forms 10
37 Information to be Logged and Tracked 11
38 Management of DR Activities Form 11
39 Disaster Recovery Event Recording 11
40 Disaster Recovery Activity Report 11
41 Mobilizing the Disaster Recovery Team 12
42 Mobilizing the Business Recovery Team 12
43 Monitoring Business Recovery Task Progress 12
44 Business Recovery Report 12
45 Communications Form 13
46 Returning Recovered Operations to Business Units 13
47 Business Process / Function Recovery Completion Form 13
48 Next Review Cycle (March 2027) 13

Information Technology Statement of Intent

This document outlines our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and telecommunications infrastructure. This summary provides recommended procedures. In an actual emergency, modifications may be made to ensure the physical safety of our people, systems, and data.

Our Mission

To ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems, and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure it can be implemented in emergency situations and that staff understand how to execute it.
- All staff must be made aware of the disaster recovery plan and their respective roles.
- The disaster recovery plan is to be kept up to date to reflect changing circumstances.

Objectives

The principal objective is to develop, test, and document a well-structured and easily understood plan to help the company recover quickly and effectively from unforeseen disasters or emergencies that interrupt information systems and business operations.

Additional Objectives:

- Ensure all employees fully understand their duties in implementing the plan.
- Ensure that operational policies are followed in all activities.
- Ensure proposed contingency arrangements are cost-effective.
- Consider the impact on other company sites.
- Establish disaster recovery capabilities for key customers, vendors, and others.

KeyPersonnel Contact Info

Name,Title	ContactOption	ContactNumber
Udaya Reddy(CTO)	Work	+91-9901833440
	Alternate	+91-9901833440
	Mobile	+91-9901833440
	Home	+91-9901833440
	EmailAddress	ub@rezolve.ai
	AlternateEmail	ub@gmail.com
Senthil Annaswamy(Director of Engineering)	Work	+91-9500071357
	Alternate	+91-9500071357

	Mobile	+91-9500071357
	Home	+91-9500071357
	EmailAddress	senthil.annaswamy@rezolve.ai
	AlternateEmail	senthil.annaswamy@rezolve.ai
Aanchal Saini (HR)	Work	+91-1352641445
	Alternate	+91-7017976615
	Mobile	+91-7906913409
	Home	+91-1352668625
	EmailAddress	Aanchal.saini@rezolve.ai
	AlternateEmail	aanchal.bharti02@gmail.com
Neil Dattani(Chief of Staff)	Work	+91-9819625281
	Alternate	+91-9819625281
	Mobile	+91-9819625281
	Home	+91-9819625281
	EmailAddress	Neil.dattani@rezolve.ai
	AlternateEmail	dattani.neil@gmail.com
Sriram (HR Admin)	Work	+91-9342509936
	Alternate	+91-9342509936
	Mobile	+91-9342509936
	Home	+91-9342509936
	EmailAddress	ssriram.manivasagam@rezolve.ai
	AlternateEmail	sriram.manivasagam@rezolve.ai

NotificationCallingTree

Person Identifying Incident

Honey Arora/Neil Dattani/Aanchal Saini/Sriram

Udaya Bhaskar Reddy/Senthil Annaswamy/Saurabh/Manish/Boopathi,

Mayank Baghel, Nagajeyanthi, Asarutheen, Muzammil, Arun Prasanth,

Sudhanshu, Shekhar Pundir, Akhilesh

Asartheen, Gopinath, Kumar raja, Muzammil, Santhosh, Aganatha, Maninathan , Shashi Ranjan,Arishanapalli, Krunal,Prasana, Kushaghra, Afnan, Vimal, waseem,Raghavendra, Vishawajeet, Tisha,Deepraj, shekhar chandola, bhaskar, Vivek Thapliyal, sneha, khushboo, khushi, sakshi, Akash, Abhishek, Krishan kamal

Vigneshwaran, Iswarya, Sumit,Arun Prasanth,Aganatha, Jameel, Pushplatha, Vinitha, Paras, Himanshi,Anubhav, Rish, Ramu, Aditi, P shashi pandey, Deepak, Kavita, shivam raj

ExternalContacts

Name,Title	**ContactOption**	**ContactNumber**
Landlord/PropertyManager		
Dehradun-IMSI		
	Work	+91-135-6677444
	Mobile	+91-9412347983
	Home	
	EmailAddress	dhyan.bisht@imsiglobal.com onkar.sharma@imsiglobal.com
Chennai-NSI		
	Work	+91-9962533318
	Mobile	+91-9962533318
	Home	

	Email Address	stpchennai@nsic.co.in
Power Company		
IMSI	Work	+91-135-6677444
	Mobile	+91-9412347983
	Home	
	EmailAddress	dhyan.bisht@imsiglobal.com onkar.sharma@imsiglobal.com
Telecom Carrier1		
Doon BroadBand Ltd	Work	+91-135-6677444
	Mobile	+91-9412347983
	Fax	
	Home	dhyan.bisht@imsiglobal.com onkar.sharma@imsiglobal.com
	EmailAddress	
TelecomCarrier2		
	Work	+91-7777031159
	Mobile	+91-7777031159
	Home	
	EmailAddress	chennaihelpdesk@hathway.net
Hardware/Supplier1		
Kamal Naithani	Work	+91-9412324759
	Mobile	+91-9412324759
	EmergencyReporting	+91-9412324759
	EmailAddress	multiplecomputersolution@gmail.com
HardwareSupplier2		
Dhanasekar	Work	+91-9840270781
	Mobile	+91-9840270781
	EmergencyReporting	+91-9840270781
	EmailAddress	lakshmicomputercare@gmail.com
SiteSecurity-		
IMSI	Work	+91-135-6677444
	Mobile	+91-9412347983
	Home	
	EmailAddress	dhyan.bisht@imsiglobal.com onkar.sharma@imsiglobal.com
PowerGenerator-		
IMSI	Work	+91-135-6677444
	Mobile	+91-9412347983
	Home	
	EmailAddress	dhyan.bisht@imsiglobal.com onkar.sharma@imsiglobal.com

Production-Server		
	Work	+1(800)6427676
	Mobile	+1(800)8925234
	Home	
	LinkAddress	https://azure.microsoft.com/en-in/support

External Contacts Calling Tree
Udaya Bhaskar Reddy
Sriram
Aanchal
Internet / Power / Lakshmi Computers
Microsoft
NSIC Premises
Internet / Power / Multiple Computers / Con
IMSI Premise / 91 Springboards / Awfis Space

1. Plan Overview

Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan, they are to be fully tested and appropriate amendments should be made to the training materials.

Plan Documentation Storage

Copies of this Plan (shared drive on Microsoft Azure) and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued location of shared drive and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued shared drive location and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

Backup Strategy

Rezolve.ai is using the Microsoft Azure services cloud services for server and hosted on https://azure.microsoft.com/en-us/overview/trusted-cloud. Company has defined the below frequency for backup.

- Server Data: Daily Differential, Weekly Full
- Process Data: Daily Differential (Domain Users and Online Users)
- Client Data: Daily Differential, Monthly Full
- Monthly Full (All Users including Offsite Users)

Rezolve.ai has provided the laptop to each employee and daily data backup is scheduled to be taken on Microsoft Azure shared drive.

Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

PotentialDisaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & RemedialActions
Flood	3	2	No critical equipment is there in the office

Fire	3	2	Fire and smoke detectors are there
Tornado	1		
Electrical storms	1		
Act of terrorism	1		
Act of sabotage	1		
Electrical power failure	3	2	Rezolve.ai has taken premise in IMSI building which has power backup monitored 24/7.
Loss of communications network services	2	2	Every employee has dongle to connect to internet from any where and start supporting the business from home.
Downtime from Cloud provider	3	4	When servers and DB are down the impact of service availability is quite high. Recovery of DB and AKS quickly is a must.Taking the backup of db in a different region is being planned this month

Probability: 5 = Very High, 1 = Very Low
Impact: 5 = Total destruction, 1 = Minor annoyance

1 Emergency Response

Alert, escalation and plan invocation

Plan Triggering Events
Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

Assembly Points
Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

- Primary - Far end of main parking lot;
- Alternate - Parking lot of company across the street

Activation of Emergency Response Team
When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

Disaster Recovery Team
The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 1.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.;
- Report to the emergency response team.

Emergency Alert, Escalation and DRP Activation
This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications

can be quickly established while activating disaster recovery.
The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

Emergency Alert
The person discovering the incident calls a member of the Emergency Response Team in the order listed:
Emergency Response Team:

- Udaya Reddy (+91-9901833440)
- Saurabh Kumar (+1-4152542699)
- Manish Sharma (+1-5103965652)
- Senthil Annaswamy (+91-9500071357)
- Aanchal Saini (+91-7906913409)
- Neil Dattani (+91-9819625281)

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.
One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

DR Procedures for Management
Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

Contact with Employees
Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

Alternate Recovery Facilities / Hot Site

1. ERT and DRT will inform the team via mobile or leaving the recorded message to connect from home or hotel and resume the business immediately.

2.3.8 Personnel and Family Notification
If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

2 Media

Media Contact
Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

Media Strategies

1. Avoiding adverse publicity
2. Take advantage of opportunities for useful publicity
3. Have answers to the following basic questions:
    - What happened?
    - How did it happen?
    - What are you going to do about it?

Media Team

- Udaya Reddy (+91-9901833440)
- Saurabh Kumar (+1-4152542699)
- Manish Sharma (+1-5103965652)
- Senthil Annaswamy (+91-9500071357)

Rules for Dealing with Media
Only the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media team.

3 Insurance

No company insurance as it is premise vendor responsibility to insure the commercial space. All the office space renovation will be taken care by IMSI.

4 Financial and Legal Issues

Financial Assessment
The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of checkbooks, credit cards, etc.
- Loss of cash

Financial Requirements
The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

Legal Actions
The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

5 DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. Rezolve.ai plan is to do DRP exercise annually. In a DRP exercise no one passes or fails; everyone who participates learns from exercises — what needs to be improved, and how the improvements can be implemented.
Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.
Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times.
The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

Appendix A – Suggested Forms

All the following items should be tracked in **Jira tickets** for DR incidents. Each ticket should include the information below for audit, tracking, and analysis purposes.

Information to Be Logged and Tracked

1. **Business or Technology Service Affected**
    - Include details of impacted services, systems, or functions.
2. **Damage Assessment**
    - Description of the extent and nature of the damage.
3. **Recovery Plan and Runbook**
    - Document the specific steps taken and recovery protocols followed.
4. **Disaster Recovery (DR) Team Mobilization**
    - List members involved and dates/times mobilized.
5. **Business Recovery Team (BRT) Mobilization**
    - List of business recovery team members and mobilization dates.
6. **Communication Plan**
    - **On Event:** Notification to stakeholders at the time of incident.
    - **On Recovery Completion:** Notification to confirm full restoration.
7. **Recovery Timing and Progress**
    - Start and end time of recovery activities.
    - Recovery task assignees, task progress, and status.
    - Outcome of recovery and any follow-up actions required.

Management of DR Activities Form

- All DR activities must be structured and recorded systematically.
- The plan must be updated continuously throughout the disaster recovery period.
- All actions taken must be recorded and tracked by the DR team.

Disaster Recovery Event Recording

- All key events must be logged by the DR team leader.
- The event log begins at the start of the emergency and is transferred to the Business Recovery Team once the initial phase is complete.

Disaster Recovery Activity Report

Prepared by the **DR Team Leader** after the initial response phase is completed. It must include:

- Description of the incident or emergency.
- Notification log (who was notified and when).
- Actions taken by the DR team.
- Outcomes of those actions.
- Impact on normal business operations.
- Assessment of BCP effectiveness.
- Lessons learned.

Distributed to:

- Business Recovery Team Leader
- Senior Management (as appropriate)

Mobilizing the Disaster Recovery Team

After a disaster is declared and damage assessed, use this format to document:

- Time of activation
- Team members contacted
- Responsibilities assigned

Mobilizing the Business Recovery Team

After DR activation, the BRT should be mobilized using a similar tracking format:

- Time of activation
- BRT members contacted
- Areas/functions covered

Monitoring Business Recovery Task Progress

- All recovery tasks must be tracked for status and interdependencies.
- Tasks should be prioritized but may run concurrently where possible.
- Ensure resourcing is sufficient and any bottlenecks are addressed quickly.

Business Recovery Report

Prepared by the **Business Recovery Team Leader** upon completion of recovery.

Contents:

- Description of the incident
- People notified and corresponding dates
- Actions taken by the BRT
- Outcomes of those actions
- Impact on operations
- Problems identified
- Suggestions to improve DR/BCP
- Lessons learned

Distributed to:

- Senior Management
- DR and Business Continuity stakeholders

Communications Form

Ensure accurate and timely communication throughout the DR/BR period. Only **authorized personnel** should engage with external communications or media.

Communication Coordination Table:

Group Affected	Coordinator Name	Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Stakeholders			
Others			

Returning Recovered Operations to Business Units

Once operations are stable:

- Handover responsibility to relevant business unit leadership.
- Formalize the transition to ensure alignment and clarity.

- Business units must sign off on restoration readiness.

Business Process / Function Recovery Completion Form

For each recovered process:

- Document signoff between the business unit leader and the BRT.
- Include details of what was restored, by whom, and when.
- This confirms readiness to resume business-as-usual operations.

NOTE – Next review cycle for this policy is March-2027. Management can review policy any time and can make changes depending on the situation.

- All documents related to policies and procedures – any reference to Actionable Science is as good as Rezolve.ai.