

BCP and DR Process

Version 10



Document Information

Name of the document	BCP and DRProcess
Release date	19-Dec-18
Owned by	Mayank Baghel
Governedby	Mr.Udaya Bhaskar Reddy

RevisionHistory

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	28-Aug-2020	Updated Retention data for 6years
4	15-Dec-2020	Reviewed and no change
5	02-Dec-2021	Reviewed and no change
6	04-Mar-2022	Updated Document Information
7	07-Mar-2023	Reviewed and no change
8	12-July-2024	Updated Document Information
9	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
10	29-May-2026	Reviewed and updated

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	02-June-2026

Table of Contents

1. Purpose and Scope	5
2. Key Personnel Contact Information	6
3. Plan Overview	7
4. Risk Management	8
5. Emergency Response	8
6. Media	11
7. Financial and Legal Issues	11
8. DRP Exercising	12

Purpose and Scope

Purpose

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

Our mission is 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 that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

- The principal objective of the disaster recovery program is to develop, test, and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:
- The need to ensure that all employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.
- The need to ensure that proposed contingency arrangements are cost-effective.
- The need to consider implications on other company sites.
- Disaster recovery capabilities as applicable to key customers, vendors, and others.

Scope

- This policy covers logical and physical boundaries of Rezolve.ai.
- This policy covers all Rezolve.ai Network, Operations area, IT systems, data and authorized users, Public users within logical and physical boundaries.

Key Personnel Contact information

Name	EmailID	ContactNumber
Udaya Bhaskar Reddy(Co-Founder & CTO)	Ub@rezolve.ai	+91-9901833440
Saurabh Kumar(Co-Founder & CEO)	saurabh@rezolve.ai	+1-415-2542699
Senthil Annaswamy(Director Engineering)	senthil.annaswamy@rezolve.ai	+91-9500071357
Aanchal Saini(Associate Manager-HR)	Aanchal.saini@rezolve.ai	+91-7906913409
Neil Dattani(Chief of Staff)	Neil.dattani@rezolve.ai	+91-9819625281

External Contacts

A list of emergency contacts will be maintained up to date and displayed in prominent locations for use by first responders and the Emergency Response Team

Name	ContactOption	ContactNumber
Fire	Phone	101

Police	Phone	100
Hospital	Phone	01352659355
Women Helpline	Phone	1091
Ambulance	Phone	102
Cyber Security	Phone	1930 0135-2655900
Disaster Management Service	Phone	108 0135-2726066

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. This will involve the use of formalized change control procedures under the control of the IT Head.

Plan Documentation Storage

Copies of this Plan, Electronic Copy, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued an Electronic Copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued an Electronic Copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

Backup Strategy

- Key business processes and the agreed backup strategy for each are listed below:
- Rezolve.ai uses standard cloud provider MS Azure for all of its offerings for both production systems and the non-production systems. The cloud offers standard backup strategy for all storage accounts, databases. Rezolve.ai has subscribed to that.

Schedule Backup Process

- & As configured by the Infrastructure team on MS Azure. The full backups of the databases are set and stored for 7 days.

Retention period Schedule for Data:

- & Full(Daily)-7days

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.

Business Impact Assessment:

expected disturbance duration on a scale from 0 to 3. Description	Event Likelihood	Anticipated Impact	Disturbance Duration
	0-NoRisk	0- _NoDisruption	0 -Minimal
	1-MinimalRisk	1-MinorDisruption	1-Upto1Day

	2- SignificantRisk 3 -Prevalent Risk	2- ModerateDisruption 3-FullDisruption	2-Upto1Week 3-Morethan1Week
Natural Threats			
Storm	1	1	0
Flood	2	1	1
Earthquake	2	0	0
Fire	1	2	1
Human Threats			
Hacking	1	1	1
Explosion	1	2	2
Riots/Civil disturbances	0	0	0
Terrorism	1	1	1
Disease epidemic/quarantines	1	2	1
Government legislation/laws/orders	0	0	0
Technical Threats			
Power outage	1	0	0
Network down	2	2	1
Communication breakdown	1	1	1
Systems interruption	1	1	1

Azure Region availability

- Resolve does not use region-redundant databases and thereby has a region outage risk.
- **Virtual Machines:** Azure provides a 99.9% uptime SLA for single-instance Virtual Machines using premium storage. For Virtual Machines in an availability set, the SLA is 99.95%. When using availability zones, the SLA increases to 99.99%.
- **Storage:** For Azure Storage, the SLA for read access to geo-redundant storage (RA-GRS) is 99.99%.
- **SQL Database:** Azure SQL Database guarantees a 99.99% availability SLA.
- **App Service:** For Azure App Service, the SLA is 99.95% for a single instance, and 99.99% for multiple instances across different regions.
- Resolve has not opted for geographic redundancy as of now. However, it hosts servers in the US, EU, and Canada regions of Azure.
- There is a rare but small chance of a region being unavailable for a certain duration.
- Resolve plans to implement data redundancy across regions during 2025.

Emergency Response

Alert, escalation and plan invocation

Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the Disaster Recovery Plan are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building (e.g., earthquake)

Assembly Points

Where the premises need to be evacuated, the DRP invocation plan identifies the following evacuation assembly point:

Assembly Point

Ground Floor,

DoonExpressBusinessPark,Suite1304,1000Building,Dehradun248001,Uttarakhand.

Module # 213 & 214, NSIC STPComplex, B-24 Guindy Industrial Estate Ekkadathangal Chennai,Tamil Nadu, 600032.

Activation of Emergency Response Team

Emergency Response Team (ERT) Activation

When an incident occurs, the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the Disaster Recovery Plan (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 include:

- 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 the disaster recovery team to maintain vital services and return to normal operations
- Ensure employees are notified and allocate responsibilities and activities as require

Disaster Recovery Team

The team will be contacted and assembled by the Emergency Response Team (ERT). The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 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 the 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

- & The Emergency Response team will consist of the key personnel as listed above
- & 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.

Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

Recorded Messages/Updates

For the latest information on the disaster and the organization's response, staff members can call a toll-free number of the company. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

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.

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

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

Media Team

The Head of marketing will handle all media queries and will be the authorized representative of the company to deal with the media.

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.

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.

DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails. All who participate learn from the exercise about what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and are confident of 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.

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 labs Private Limited is as good as Rezolve.ai