Retirebest

Disaster Recovery Plan

DISASTER RECOVERY PLAN

for

RETIREBEST (PTY) LTD

registration number: 2022/244873/07

Introduction

This policy consists of the rules procedures that we will follow when IT services are disrupted including as a result of a natural disaster, technological failure or human factors such as hacking, sabotage or political disruption. The policy is designed according to the principle of restoring the affected business processes as quickly as possible, either by bringing disrupted services back online or by switching to a contingency system.

Purpose and Scope

The purpose of this policy is to:

- minimise interruptions to the normal operations.
- limit the extent of disruption and damage.
- minimise the economic impact of the interruption.
- establish alternative means of operation in advance.
- train personnel with emergency procedures.
- provide for smooth and rapid restoration of service.

This policy must be read together with all of Retirebest's company polices.

Contact Tree

These are the key resources involved in the disaster recovery plan, including all key stakeholders and third-party resources.

Name	Role	Phone	Email	Contacting
Neil Botha	Director	+27 84 504 0505	neil@retirebest.co.za	- Alan Rainnie - Michael du Toit
Alan Rainnie	Director	+27 82 4971501	alan@retirebest.co.za	- Neil Botha - Michael du Toit
Michael du Toit	IT Head	+27 66 4473124	michael@retirebest.co.za	- Neil Botha - Alan Rainnie

Information Services Backup Procedures

1. Client digital assets

Daily: Database encrypted backups, saved onto a secure AWS S3 bucket with a 30 day retention period. These backups are encrypted using AES-256 encryption. Backups are triggered and processed by AWS infrastructure that is provided with the RDS database service. All RDS database backup events are logged automatically.
Source Code: Source and environment recovery scripts are stored off-site on Gitlab. Gitlab is a git-based cloud storage service for storing code.

2. Personal Computer

Company-related data is stored on Google Drive folders on all personal computers. These folders are synched to Google Cloud in real-time.
All employees and users of our systems are instructed to save any work-related items to the designated folders on the local drive as directed by a senior Retirebest staff member.

Disaster Recovery Procedures

In the event of an emergency including fire, natural disaster or other life/security threatening event, the following steps are taken:

1. Initiate the DRP

Notify relevant personnel via the call list
Determine degree of disaster
Implement application recovery plan depending on extent of disaster
Monitor progress
Notify affected users (if applicable)

2. Follow up on DRP implementation

List teams and tasks of each
Set up the delivery and the receipt of mail
Establish emergency office supplies
Rent or purchase equipment, as needed
Determine applications to be run and in what sequence
Identify number of workstations needed
Set up primary vendors for assistance with problems incurred during emergency
Plan for transportation of any items needed at backup site
Take copies of system and operational documentation and procedural manuals.
Ensure that all personnel involved know their tasks
Notify insurance companies

Restoration Process

Our production environment is fully scripted, and the script is stored in source control. We can script and relaunch our environment in the event of a disaster.

Step 1: Run CloudFormation script to generate database environment
Restore database data from latest backup on S3 bucket

Step 2: Run CloudFormation script to generate production environment

Step 3: Test environment

Recovery Plan Practice and Exercising

Generate duplicate database environment
Restore latest database backup
Generate duplicate production environment from source control
Test and validate application against latest database backup in new environment
Tear down duplicate environment once testing complete

DRP History

Version No.	Approved by	Signature/Revision date	Key changes
1	Neil Botha		-