



GHT (PTY) LTD — BUSINESS CONTINUITY PLAN

1. PLAN INTRODUCTION

1.1 Introduction

The Business Continuity Plan aims to ensure that in the event of an operational, technical, or environmental disruption to the FSP, essential systems, procedures, data, and services are preserved, and regulated activities are maintained with minimal disruption.

A crisis event is defined as any disaster or incident—natural, technological, or operational—that threatens or halts daily operations. Crisis events may stem from:

- Natural disasters (e.g., fires, floods).
- Malicious actions (e.g., cyberattacks, physical breaches).
- Technological breakdowns (e.g., hardware failure, database corruption, prolonged network outages).
- Staff disruptions (e.g., unexpected loss of key personnel).

1.2 Purpose

- Ensure the continuity of core business operations during a disruption.
- Maintain data integrity and strict system security under disaster recovery protocols.
- Minimize client prejudice, financial loss, regulatory exposure, and reputational risk.
- Provide our underwriting partners and insurers with verifiable assurance regarding technical resilience and data preservation.

2. DEFINITIONS

- **"Business Continuity"**: The capability of the organization to maintain service delivery at predefined acceptable levels during and after an incident.

- **"Core Business Functions"**: Essential operations required to deliver financial services and administer policy portfolios.
- **"GHT"**: GHT (Pty) Ltd, an authorized financial services provider incorporated in South Africa.
- **"RPO (Recovery Point Objective)"**: The maximum acceptable age of data loss preceding an outage (2 hours for databases; 12 hours for file assets).
- **"RTO (Recovery Time Objective)"**: The targeted duration of time within which business systems must be restored following an approved disaster declaration.

3. RESPONSIBLE PERSONS & EMERGENCY CONTACTS

- **Approval & Monitoring**: Nicole du Plooy (Managing Executive) & GHT Management Team.
- **Technical Implementation & DR Execution**: Werner Fettke (IT & Systems Management).

Name & Surname	Role / Area	Contact Details
Nicole du Plooy	Executive Management, Compliance & Governance	073 345 3926
Werner Fettke	IT, Security, DR Infrastructure & Systems Management	082 411 9202
Ulrich van Heerden	Financial Management	083 229 7205
Elisma Pretorius	Administration, QLink & Key Account Management	083 287 1880
Monja Anderson	Key Account Management and Head of Learnership	0833847430

4. TECHNICAL DISASTER RECOVERY (DR) INFRASTRUCTURE

To mitigate single-point-of-failure vulnerabilities and guarantee high availability, an isolated, dedicated DR server environment has been deployed.



4.1 System Endpoints & Encryption

The DR environment is hosted on dedicated secondary infrastructure and secured via end-to-end SSL/TLS encryption certificates:

- **GHT Connect DR Portal:**
https://dr.ghconnect.co.za/
- **Informal Market DR Portal:**
https://dr.informalmarket.co.za/

4.2 Automated Backup & Synchronization Cycles

- **Database Layer:** Automated, transactional database backups run from the production environment to the DR database server every **2 hours** (Maximum Database RPO = 2 hours).
- **Application & Media Layer:** System application code, uploaded client documentation, recorded call audio files, and system artifacts synchronize from production servers to the DR server every **12 hours** (Maximum Media RPO = 12 hours).

5. DR ACTIVATION & FAILOVER GOVERNANCE

The DR environment operates strictly in a standby/backup capacity to preserve data integrity and prevent out-of-sync operational records.

5.1 Failover Threshold (When DR is Activated)

- **Standard / Minor Incidents:** Temporary power/network outages, local ISP interruptions, or minor technical issues resolvable within a standard window (e.g., under 1 to 2 hours) **shall not** trigger DR activation. Operations will remain on the production environment to prevent data recreation overhead.
- **Catastrophic / Extended Incidents:** Failover to the DR portals (dr.ghconnect.co.za / dr.informalmarket.co.za) is triggered **only** upon declaration of an extended critical disaster (e.g., catastrophic hardware failure, unrecoverable data center compromise, or sustained multi-day production downtime).

5.2 Failover Decision Protocol

1. **Incident Triage:** Werner Fettke assesses system downstate and estimated restoration time.
2. **Executive Authorization:** If downtime will exceed acceptable thresholds, Nicole du Plooy (or designated alternate) authorizes switching operational traffic to the DR instances.



3. **Cutover:** Staff are directed to log in via the secure DR URLs. The DR database at the point of last synchronization becomes the active transactional ledger ("The Gospel").

5.3 Failback & Data Reconciliation Protocol (Post-Incident)

When the primary production environment is fully restored and verified secure:

1. **Freeze DR Access:** Administrative lock applied to DR portals to prevent new transactional entries.
2. **Reverse Synchronization:** The active DR database state and all uploaded documents/call logs generated during the DR period are synchronized back to the primary production servers.
3. **Data Audit:** Werner Fettke verifies checksums and transactional integrity.
4. **Resumption:** Traffic is routed back to standard production URLs, and DR returns to passive standby synchronization.

5. MINIMUM OPERATIONAL REQUIREMENTS & KEY RESOURCES

6.1 Core Business Functions

Priority	Core Function	Responsible Person(s)
1	Financial, Compliance, Operational & Executive Management	Nicole du Plooy
2	IT Infrastructure, DR Systems, Security & Data Backup	Werner Fettke
3	Administration, QLink Integration & Underwriter Liaison	Elisma Pretorius
4	Key Individual Regulatory Oversight	Michael du Plooy
5	Project & Portfolio Management	Monja Anderson



6.2 Key Resource Redundancy

Key Resource Role	Primary Person	Alternative Resource
Financial Management	Nicole du Plooy	Ulrich van Heerden / Michael du Plooy
Operational & Policy Admin	Elisma Pretorius	Monja Anderson
IT & DR Systems	Werner Fettke	Lionel Smith (Technical Support Escrow)

6. TESTING, AUDITING & GOVERNANCE COMPLIANCE

- **Semi-Annual DR Replication Verification:** Bi-annual verification of the automated 2-hour database backups and 12-hour media sync jobs to ensure zero archive corruption.
- **Simulated Failover Walk-Through:** Annual dry-run testing of the DR web portals and rollback procedures with key administrative personnel.
- **Regulatory & Governance Alignment:** Maintained in accordance with King V governance principles and insurer data security requirements, ensuring ongoing business resilience and data confidentiality.

Approved by: Nicole du Plooy



Director / Compliance Officer of GHT

Date of Approval: 20 August 2026

