IshemaLink National Logistics Platform

Disaster Recovery Plan

Version 1.0 | Rwanda Data Center (AOS/KTRN) | 2026

Document	IshemaLink Disaster Recovery Plan
Author	Carine Umugabekazi
Classification	Confidential — Internal Use Only
Date	February 2026
Version	1.0
Review Cycle	Quarterly

1. Executive Summary

This Disaster Recovery Plan (DRP) defines the procedures, responsibilities, and timelines for restoring IshemaLink's national logistics platform following any disruptive event. IshemaLink processes financial transactions, government compliance records, and cargo manifests for Rwanda's national logistics network. Any extended downtime results in direct economic impact to agents, drivers, exporters, and government oversight bodies including RURA and RRA.

This plan targets a Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour for all critical services, ensuring compliance with Rwanda's data sovereignty requirements and MINICOM's national rollout conditions.

Recovery Objectives

Service	RTO	RPO	Priority
PostgreSQL Database	2 hours	1 hour	Critical
Django/Gunicorn API	1 hour	N/A (stateless)	Critical
Redis Cache/Queue	30 minutes	15 minutes	High
Celery Workers	1 hour	N/A	High
Nginx/SSL	30 minutes	N/A	Critical
Prometheus/Grafana	4 hours	N/A	Medium

2. Risk Assessment

Risk Event	Likelihood	Recovery Action
Server Hardware Failure	High	Immediate failover to standby server. PostgreSQL restored from MinIO backup.
Database Corruption	Medium	Restore from last automated backup (max 1 hour data loss). PgBouncer disconnects cleanly.
Network / Internet Outage	High	Rwanda-specific: 4G outages in districts. Mobile agents use offline sync. API remains available
Power Outage at AOS/KTRN	Medium	Data center has UPS and generator backup. Docker containers restart automatically on power
Docker Container Crash	High	All containers configured with restart: always. Auto-restart within 30 seconds.
Ransomware / Cyberattack	Low	Restore from clean MinIO backup. Debug=False prevents information exposure.
Accidental Data Deletion	Medium	Point-in-time recovery from automated daily backups retained for 30 days.

3. Backup Strategy

3.1 Automated Daily Backups

The backup.sh script runs daily at 02:00 AM via cron job on the production server. It performs a full PostgreSQL dump and uploads to MinIO (self-hosted within Rwanda). Local copies are retained for 7 days.

Backup Schedule:

Frequency	Type	Retention	Storage
Daily (02:00 AM)	Full DB dump (pg_dump)	30 days	MinIO (Rwanda)
Weekly (Sunday)	Full system snapshot	12 weeks	MinIO (Rwanda)
Real-time	PostgreSQL WAL logs	24 hours	Local server

3.2 Data Sovereignty Compliance

All backups are stored on MinIO hosted within Rwanda's borders (AOS or KTRN data center). No backup data leaves Rwanda. This satisfies MINICOM's data sovereignty requirement for the national rollout.

4. Disaster Recovery Procedures

4.1 Complete Server Failure

1. Provision new Ubuntu 22.04 server at AOS/KTRN data center.
2. Install Docker and docker-compose (see DEPLOYMENT.md).
3. Clone ishemalink_api repository from GitHub (main branch).
4. Configure .env.prod with production credentials.
5. Download latest backup from MinIO: aws s3 cp s3://ishemalink-backups/latest.sql /tmp/
6. Start database container only: docker-compose -f docker-compose.prod.yml up -d db
7. Restore backup: cat /tmp/latest.sql | docker exec -i db psql -U ishema -d ishemalink
8. Start all services: docker-compose -f docker-compose.prod.yml up -d
9. Verify health: curl https://your-domain.com/api/status/
10. Notify stakeholders — system restored.

4.2 Database Corruption Only

1. Stop web and worker containers to prevent further writes.
2. Identify last clean backup timestamp from MinIO.
3. Restore: docker exec -i db psql -U ishema -d ishemalink < backup.sql
4. Verify data integrity: docker-compose run web python manage.py check
5. Restart all services.

4.3 Container Crash (Auto-Recovery)

All Docker containers are configured with restart: always in docker-compose.prod.yml. A crashed container automatically restarts within 30 seconds without manual intervention. Prometheus alerts notify the on-call engineer if a container fails to restart after 3 attempts.

4.4 Rwanda Network Outage (Nyamagabe / Rural Districts)

IshemaLink is designed for intermittent connectivity. During a district-level network outage:

- Mobile agents: app queues shipment requests locally and retries when connectivity returns.
- Drivers: receive last-known assignment via SMS (delivered when network restores).
- API server: continues serving agents with connectivity. No data is lost.
- Government integrations: RURA/RRA calls are queued via Celery and retried automatically.
- Target: full sync within 15 minutes of connectivity restoration.

5. Recovery Roles and Responsibilities

Role	Responsibility	Contact
Lead Engineer	Execute recovery procedures, coordinate restoration	Carine Umugabekazi
Data Center (AOS/KTRN)	Hardware provisioning, network restoration	AOS Rwanda NOC
Database Admin	Backup restore, data integrity verification	DBA on-call
Government Liaison	Notify RRA/RURA of service interruption	GovTech contact

6. Communication Plan

During a disaster event, stakeholders are notified in the following order within the first 30 minutes:

1. Internal team notified via SMS broadcast (NotificationEngine).
2. MINICOM and RURA notified of service interruption via official email.
3. Active agents notified via SMS: 'IshemaLink is temporarily unavailable. Your data is safe.'
4. Status updates every 30 minutes until restoration.
5. Post-incident report sent to all stakeholders within 24 hours of restoration.

7. Testing and Review

This disaster recovery plan is tested quarterly through simulated failure scenarios. Each test validates backup restoration time, container auto-restart behavior, and network outage handling. The plan is reviewed and updated after each test and after any significant infrastructure change.