

Disaster Recovery and Business Continuity Plan (Summary)

Document ID: IE-DRP-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: IT & Engineering - Infrastructure

1. Objective

To ensure the continuity of critical business functions and rapid recovery of the SaaS platform following any major disruption (natural disaster, regional outage, cyber-attack).

2. Key Recovery Metrics

Metric	Definition	Target Time
RPO (Recovery Point Objective)	Maximum acceptable data loss (time between last consistent backup and failure).	15 minutes (for core production data).
RTO (Recovery Time Objective)	Maximum acceptable time to restore critical business functions after a disaster is declared.	4 hours (for core SaaS platform functionality).

3. Recovery Strategy

- Criticality:** Tier 0 (Core AI Inference, API Gateway, Authentication) is prioritized. Tier 1 (Analytics, secondary services) follows.
- Data Backup:** All production database data is backed up continuously (RPO 15 min) and replicated asynchronously to the designated **DR Region (Europe)**.
- Failover Mechanism:** The Primary Region uses a **Pilot Light** strategy. In the event of primary failure, the DR region's standby compute resources can be scaled up and pointed to the replicated data to meet the RTO target.
- Testing:** Full disaster recovery simulation (failover to DR region and back) must be performed **semi-annually**. Results are reported to the CTO.

4. Business Continuity (BC)

- **Personnel:** The **Remote Work Policy** ensures continuity of operations as all staff are already distributed.
- **Vendors:** Critical third-party vendors must have documented DR plans and be reviewed annually via the **Vendor Due Diligence Form**.