# BDI Business Portal – Data Backup and Recovery Policy

Effective Date: September 2025

Approved By: Office of the CTO

Applies To: Boundless Devices Inc. (BDI) Business Portal production systems, staging environments, and associated storage

## 1. Purpose

The purpose of this policy is to ensure the confidentiality, integrity, and availability of data within the BDI Business Portal through a defined backup and recovery strategy. This policy establishes standards for protecting both the PostgreSQL database layer (Supabase-managed) and the object storage layer (Supabase Storage), including associated metadata and directory files.

## 2. Scope

This policy applies to all production data residing in the BDI Business Portal, including:  
- PostgreSQL databases and schemas managed through Supabase.  
- Metadata associated with authentication, roles, and policies.  
- Supabase Storage files and directories, including organization documents, uploaded assets, and other binary objects.  
- Infrastructure and CI/CD backups related to Supabase deployments.  
  
This policy does not apply to non-production sandbox environments or developer local instances, except where explicitly designated.

## 3. Backup Components

### 3.1 Database (PostgreSQL – Supabase Managed)

- Point-in-Time Recovery (PITR): Enabled for production, allowing recovery to any point within the retention window.  
- Schema Dumps: Weekly logical backups (`pg\_dump`) stored for schema version tracking.  
- Coverage includes tables, views, indexes, RLS policies, functions, triggers, sequences, and authentication metadata.  
- Exclusions: Storage API files are not included in PITR.

### 3.2 Storage Files (Supabase Storage)

- Supabase PITR covers only metadata, not actual file objects.  
- Automated nightly sync via rclone to Google Drive:  
 rclone copy supabase:organization-documents \  
 gdrive:SupabaseBackups/organization-documents \  
 --progress \  
 --s3-endpoint https://<project-ref>.storage.supabase.co/storage/v1/s3 \  
 --s3-force-path-style \  
 --s3-no-check-bucket \  
 --disable-http2  
- Retention: Daily (30 days), Weekly (6 months), Monthly (7 years).

## 4. Backup Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Frequency | Retention | Method |
| Database PITR | Continuous | 14 days (default) | Supabase physical backups + WAL |
| Schema Dumps | Weekly | 12 months | pg\_dump via CI/CD |
| Storage Files | Daily (incremental) | 30 days / 6 months / 7 years | rclone to Google Drive |

## 5. Recovery Procedures

5.1 Database:  
- Recovery from PITR initiated via Supabase Dashboard.  
- Target timestamp selected within retention window.  
- Post-recovery validation of schema and RLS policies required.  
  
5.2 Storage Files:  
- Restore via reverse rclone sync from Google Drive.  
- Validate against metadata table entries.  
  
5.3 Combined Recovery:  
- Order: Database → Metadata Validation → Storage Restore → Application Rollout.  
- Post-restore audits include checksum verification and database consistency checks.

## 6. Roles and Responsibilities

- CTO: Policy owner.  
- DevOps Lead: Executes and monitors backups.  
- Data Protection Officer: Reviews logs, ensures compliance.  
- Engineering Team: Conducts biannual recovery drills.

## 7. Monitoring and Reporting

- Backup logs aggregated from rclone and Supabase PITR.  
- Failures trigger Slack alerts.  
- Quarterly verification of integrity with test restores.

## 8. Limitations

- PITR does not cover deleted Supabase Storage files, only metadata.  
- Google Drive is primary offsite; secondary provider evaluation ongoing.  
- Large restores may introduce delays.

## 9. Policy Review

This policy will be reviewed annually or upon Supabase platform changes. Updates must be approved by the CTO and documented in the Policy Revision Log.