

BUSINESS CONTINUITY & DISASTER RECOVERY PLAN

What happens when something goes very wrong.

Version history: v1.0 — 25 October 2026 (initial publication). v1.1 — 25 October 2026 (audit fixes).
See [/legal/CHANGELOG.md](#)

This Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DRP") describes how DigiSurvey remains available, and how we restore service after a disruption. It covers Recovery Time Objective (RTO) and Recovery Point Objective (RPO), the backup strategy, the planned secondary region, succession of control, the scenarios we have thought through, how often we test, and how we communicate during an incident.

This page is written for insurer InfoSec questionnaires and for your own records. If a specific insurer MSA requires us to attach it as a schedule, we will.

1. Scope

- All **customer-facing services**: the DigiSurvey web application, the mobile applications once published, the public APIs, authentication, PDF generation, and the OCR pipeline.
- The **data layer**: the primary Supabase Postgres database (ap-south-1), Supabase Storage objects, and Cloudflare R2 object storage.
- The **support operation**: ticketing, on-call, insurer-facing communication, Grievance Officer contactability.
- The **governance**: Director decision-making, Grievance Officer availability, access to banking and payroll — so the business survives even if a Director is temporarily unavailable.

2. Objectives: RTO & RPO

Function tier	Examples	RTO (Recovery Time)	RPO (Recovery Point)
Critical	Login, survey creation, survey retrieval, insurer sync, authentication	4 hours	24 hours (last successful daily backup)
Secondary	Reporting dashboards, analytics, bulk exports, marketing site,	24 hours	24 hours

Function tier	Examples	RTO (Recovery Time)	RPO (Recovery Point)
	Knowledge Hub		
Internal	Admin tooling, support ticket back-office, finance tools	72 hours	24 hours

Where live replica (Clause 4) is in place, effective RPO improves toward near-zero. The 24-hour RPO is the **worst-case contractual commitment**, not the typical performance.

3. Backup strategy

- **Nightly encrypted database dump** — a full PostgreSQL dump is taken each night from Supabase (ap-south-1), GPG-encrypted (AES-256) with a passphrase held only by Digitaliisla, and written to Backblaze B2 in a separate region. [Live](#)
- **Three-way media storage** — every survey photo, document and PDF lives in **three independent clouds simultaneously**: (1) Supabase Storage (ap-south-1, Mumbai) — primary; (2) Cloudflare R2 — hot-tier edge-cached delivery; (3) AWS S3 Mumbai (ap-south-1) — India-resident archival copy. A full outage of any one storage layer leaves two complete copies intact. [Live](#)
- **Encrypted offsite backup to Backblaze B2** — database dumps + a media mirror are additionally written to Backblaze B2 (ciphertext only) as a fourth, cold-storage copy on a different cloud and different region (US). [Live](#)
- **Separate clouds, separate regions** — the backup chain uses four distinct providers (Supabase, Cloudflare R2, AWS S3, Backblaze B2) across three continents. A full compromise of credentials for any one provider cannot delete all copies of the data.
- **Retention** — **30-day rolling** for daily backups; a **monthly snapshot kept for 13 months**; one **yearly snapshot kept for 7 years** (aligned with the IRDAI 7-year retention for claim records and the Companies Act books-of-account requirement).
- **Immutability** — Backblaze B2 Object Lock is enabled on the backup bucket; a stolen credential cannot delete a backup within its lock period. [Live](#)
- **Restore verification** — a scripted test-restore of the latest nightly dump runs weekly on an isolated instance; a human reviews the result monthly.

4. Secondary region & infrastructure resilience

- **Primary region** — Supabase ap-south-1 (Mumbai) is the authoritative home of all customer data. [Live](#)

- **Cross-region replica** — a hot standby in a second AWS region (ap-southeast-1, Singapore, or ap-south-2 when generally available) will provide near-zero-RPO failover.

Planned Q2 2027

- **Cloudflare routing** — our edge is Cloudflare: an outage of our origin does not take the status page or the brand site offline, and read-only “sorry, we’re restoring” pages are served at the edge. **Live**
- **CDN failure** — if Cloudflare itself is unavailable, we fall back to a direct origin DNS record (prepared in advance) within TTL + propagation time, typically under 10 minutes.
- **Data residency during failover** — where failover crosses a region boundary (e.g. temporary read-only service from ap-southeast-1), **we notify affected insurer customers** as part of the incident communication and record the duration in the post-mortem.

5. Succession & access to recovery keys

DigiSurvey is a two-Director company. Both Directors are empowered to execute a restore on their own.

- **Mrs. Monika Sharma** (Director & Authorised Signatory) — holds a **full key envelope**: the backup-encryption passphrase, root credentials for Supabase and Cloudflare (break-glass), and the Backblaze master application key. Stored sealed, off-site.
- **Mr. Vikas Saini** (Director & Founder) — holds **an identical, independent envelope**, stored at a different physical location.
- Either Director can, on their own, authorise and execute a full restore from backups and the resumption of service. There is no requirement for both to be reachable at the same time.
- **Grievance Officer contact** — Mr. Alok Sharma can be reached under DPDPA 2023 obligations even if the Directors are temporarily unavailable.
- **Succession beyond the Directors** — in the long-term unavailability of both Directors (an outcome we treat as the worst-case scenario), the Company’s statutory auditor and the Chartered Accountant are the first points of contact, with the Grievance Officer coordinating a managed wind-down or sale consistent with insurer MSA terms.

6. Scenarios covered

Scenario	First response	Primary mitigation
Cloud provider outage (Supabase ap-south-1, Cloudflare, Backblaze)	On-call confirms the upstream status page, posts to our status page (when live), notifies insurer customers via email per Clause 8.	Degrade gracefully; wait for upstream recovery for RTO-bounded outages; when the replica is live (Q2 2027), fail over.

Scenario	First response	Primary mitigation
Data corruption (bad migration, bug, bulk delete)	Freeze writes to the affected tables; take an immediate point-in-time snapshot before the restore starts.	Point-in-time restore from Supabase daily backup; selective restore of affected rows from the GPG-encrypted dump on Backblaze.
Ransomware / malicious encryption	Isolate affected systems; preserve forensic image; convene incident response per Breach Notification SOP.	Rebuild from the most recent clean, encrypted Backblaze backup (Object-Lock immutability means the ransomware cannot have overwritten it). CERT-In 6-hour filing where applicable.
Physical disaster at HQ (fire, flood, loss of office premises)	Operations relocate to home-working; cloud operations are unaffected because nothing production-critical lives on an HQ server.	Shift support channels to on-call cellular; secondary postal address for grievance notifications in writing — served copy may be sent to legal@digitaliisla.co.in as alternative, as noted in Audit Readiness.
Key personnel incapacitation (one or both Directors)	The remaining Director assumes all operational authority; if both are incapacitated, Clause 5 succession applies.	Each Director holds an independent key envelope (Clause 5). No single person is a critical dependency.
Sub-processor failure (payment gateway down, OCR provider down, email provider down)	Communicate degraded functionality; disable the affected feature in the UI rather than crash.	Documented fallbacks: alternative payment capture for the subscription (invoice/UPI), queued OCR, delayed transactional email.
Nationwide regulatory outage (e.g. a CERT-In mandated takedown, judicial order)	Comply with the order; document the scope; notify affected customers of the specific functionality constrained.	Scope compliance narrowly as the order permits; legal counsel engaged within hours.

7. Testing & exercises

- **Tabletop exercises** — **semi-annually**, both Directors run through two scenarios (chosen fresh each half) and document decisions, delays, and improvements. The output goes into the next revision of this plan.
- **Full restore exercise** — **at least once per year**, we take the latest encrypted Backblaze backup and perform a full end-to-end restore to an isolated instance. The restore time is recorded and compared against the 4-hour RTO.
- **Weekly automated verification** — the latest nightly dump is restored to a temporary instance by a scheduled job; schema integrity and row-counts are checked; the result is logged.
- Results of the full annual exercise are available to insurer customers under NDA on request.

8. Communications during an incident

- **Status page** — `status.digitaliisla.co.in` is the first channel. **Planned Q1 2027**. Until it is live, the home page carries a banner during a declared incident.
- **Email to all registered users** — for any **declared incident** (Sev 1 or regulated breach), we send an email to the admin on each affected tenant **within 2 hours** of declaration, with: what we know, what we don't, what we are doing, and when we will next update. Updates follow every 2 hours while the incident is ongoing.
- **Insurer-specific communication** — where the incident affects a specific insurer customer, their named contact is also notified by phone.
- **Regulatory communication** — CERT-In within 6 hours where applicable; Data Protection Board within 72 hours for a Data Breach; IRDAI as the circumstances require. See Breach Notification SOP.
- **Public post-mortem** — published within **30 days** of resolution, with root cause, timeline, remediation, and what we changed to prevent recurrence.

9. Insurance

- **Cyber Liability** — covers forensic investigation, breach notification costs, regulatory fines where insurable, and third-party claims. Policy limits available to insurer legal teams on NDA.
- **Business Interruption** — covers revenue loss from a declared disaster that interrupts service beyond a defined waiting period. Limits available on NDA.
- **Directors & Officers (D&O)** — standard governance cover.
- **Professional Indemnity** — covering the Company's technology service to IRDAI-licensed surveyors under its platform.
- Insurance evidence is produced to auditors through our Audit Readiness data-room; limits are not published publicly.

10. Review & ownership

- Owner: Mr. Vikas Saini, Director (Technical) — day-to-day responsibility for the BCP.
- Approver: Mrs. Monika Sharma, Director & Authorised Signatory — signs each revision.
- Attestor: Mr. Alok Sharma, Grievance Officer — witnesses the plan and confirms grievance-handling continuity.
- Review cadence: at least semi-annually, and after every exercise or declared incident.

BUSINESS CONTINUITY COMMITMENT · SIGNED

Digitaliisla Technologies Private Limited commits to the RTO, RPO, backup regime, succession arrangements, exercise cadence, and incident communications described in this plan. Where a commitment is marked **Planned**, we commit to delivering it on the stated timeline and to notifying customers of material slippage. Where a commitment is marked **Live**, we commit that it is in place today, and that we will produce evidence to insurer customers on request under NDA.

Mrs. Monika Sharma

Director · Authorised Signatory

Mr. Vikas Saini

Director & Founder

Dated: 25 October 2026 · Jhunjhunu, Rajasthan, India

Witnessed by Grievance Officer: Mr. Alok Sharma, Advocate — Grievance Officer; Bar Council of Rajasthan, Enrolment No. R/1387/2012 · grievance@digitaliisla.co.in · +91 93145 91361

CIN U62011RJ2026PTC119030 · Registered office: Khemi Sati Road, Jhunjhunu, Rajasthan – 333001 · legal@digitaliisla.co.in