SendTax

TRUST CENTER

Business Continuity & Disaster Recovery Policy

How we keep the service available during disruption — and how we recover when something breaks.

Effective: May 21, 2026 **Owner:** Liam Howell, Co-founder, SendTax **Status**: V1.0 – initial publication

Review cadence: Semi-annual, or after any material change to infrastructure, sub-processors, or recovery capabilities, and additionally whenever a Critical or High-severity incident closes

---

1. Purpose

This policy describes how SendTax keeps the service available during disruption, what is done when a disruption becomes a disaster, and how the service recovers. It combines Business Continuity and Disaster Recovery in a single document, which is proportionate to SendTax's size and stage. This policy supports the commitments made in the **Information Security Policy** and aligns with SOC 2 Common Criteria CC7.5 (recovery from identified events) and the SOC 2 Availability Trust Services Criterion.

This is a candid description of SendTax's **current posture** at this stage. SendTax is not claiming multi-region active-active deployment, validated recovery-time objectives, or capabilities not built. Items in §11 are deliberate next steps.

2. Scope

This plan covers:

- The technical resilience of the SendTax service
- The procedures SendTax follows when a component fails or a region becomes unavailable

- Preparations for events that affect the SendTax operating team itself (key-person unavailability, loss of operator device)

It does not cover financial business continuity for Howell & Gibbs LLC as a company; that is addressed separately. Incidents that affect security but not availability are governed by the **Incident Response Policy**.

3. Definitions

Term	Meaning
BCP	Business Continuity Plan — how the company keeps critical operations running during a disruption
DRP	Disaster Recovery Plan — how IT systems, data, and infrastructure are restored after a disaster
BIA	Business Impact Analysis — prioritization of services and data by criticality
RTO	Recovery Time Objective — maximum acceptable downtime before service is restored
RPO	Recovery Point Objective — maximum acceptable data loss, measured backward from the moment of failure
PITR	Point-in-Time Recovery — restoring a database to a specific moment in time within a retention window
SPoF	Single point of failure — a component whose loss takes down the service even if redundant components elsewhere are healthy

4. Principles

- **Honesty over theater.** SendTax describes its actual recovery capabilities, not aspirational ones. Where formal targets do not yet exist, the policy says so.
- **Inherited resilience where appropriate.** SendTax runs on managed infrastructure providers whose continuity capabilities exceed what SendTax could build alone. The policy describes how SendTax depends on those capabilities rather than re-engineering them.

- **Test what you commit to.** Untested recovery is hypothesis, not capability. SendTax tests recovery on a defined cadence.
- **Single points of failure are visible.** Where SendTax has a single point of failure, the policy names it.
- **Customer communication during disruption.** Customers learn about disruptions from SendTax, not from their own debugging.

5. Business Impact Analysis

In recovery, components are restored in this priority order:

Prio	Component	Why it ranks here
P1	Database (Fly.io Managed Postgres `st-pg-prod`) and document storage (Cloudflare R2)	No other component is useful without customer data being readable
P1	Google Cloud KMS	Documents cannot be decrypted without KMS unwrap; this gates all customer-document operations
P1	Clerk (authentication)	Customers cannot reach their data without sign-in
P2	API service (`st-api-prod`)	Required for any customer interaction beyond cached pages
P2	Celery worker (`st-worker-prod`)	Required for document classification, OCR, scheduled obligations, and email fan-out — the service is degraded but partially usable without it
P3	Web apps (`st-www`, `st-filer-web`, `st-pro-web`, `st-admin-web`)	Browser-side concerns. Static content can be served from cache during a backend outage; signed-in interactions cannot
P3	Postmark	Inbound and outbound transactional email. Inbound document submission and

		account-critical email flows degrade; data remains intact
P3	Sentry, PostHog, Modal	Observability and ML inference. The service runs without them

6. Resilience controls currently in place

This section describes what is actually deployed today.

6.1 Application layer (Fly.io)

- **Primary region:** All SendTax application machines (API, workers, web frontends) run in Fly.io's `iad` region (US-East, Ashburn, Virginia). This is configured explicitly in every `fly.toml` in the repo.
- **Per-machine resilience:** Fly automatically restarts machines on health-check failure. The API service is configured with `min_machines_running = 1` and `auto_start_machines = true`; workers have `[[restart]] policy = "always"` with up to 5 retries.
- **Health checks:** `/health/` on the API and a broker-connectivity sidecar on the worker, both polled every 30 seconds by Fly.
- **Auto-rollback on deploy failure:** Failed health checks block deployments and surface in `fly checks list`.

6.2 Database layer (Fly.io Managed Postgres)

- **Managed service:** Production uses Fly.io Managed Postgres (`st-pg-prod`), which provides automatic failover and managed high availability per Fly's published terms.
- **Backups:** Automated daily backups with point-in-time recovery within the managed plan's retention window. SendTax does not maintain a separate backup pipeline.
- **Encryption:** Storage and backups are encrypted at rest by Fly's managed service.

6.3 Document storage (Cloudflare R2)

- **Durability:** R2 provides Cloudflare's published durability guarantees and geographic distribution across the Cloudflare network.
- **Encryption layers:** Documents are AES-256-GCM-encrypted by the SendTax application before upload; R2 then applies its own at-rest encryption. Customer documents are encrypted twice, with SendTax holding the key-management end of the outer layer (see **Encryption Policy**).
- **Object versioning:** *(2026-05-26 status: enabling object versioning on the production documents bucket via the Cloudflare R2 dashboard is the remaining Phase-2 task. Until the toggle is flipped, recovery from application-bug-induced or accidental deletion relies on point-in-time database recovery and the per-document AES-256-GCM envelope encryption that prevents a compromised bucket from exposing plaintext.)*

6.4 Key management (Google Cloud KMS)

- **Managed service:** KEK custody is in GCP Cloud KMS, region `us-east1`. KMS is operated by Google and inherits its SLA.
- **Authentication:** Workload Identity Federation; no long-lived service-account keys on application servers.
- **Dual-key migration path:** The encryption module supports pointing wrap operations at a new KEK while still being able to unwrap DEKs that were wrapped under a legacy KEK — usable as a rolling re-encryption path during a key rotation or compromise (see **Encryption Policy** §8). *(Verified 2026-05-26: `st-backend/app/core/encryption.py` lines 118-125 document the optional `secondary_key_name` parameter, and lines ~191-222 implement `_unwrap_with_fallback` — wrap always uses the primary key, unwrap tries primary then secondary on `INVALID_ARGUMENT`, and `rotate_document_dek` re-wraps lazily.)*

6.5 Identity (Clerk)

- **Managed service:** Authentication is delegated to Clerk, which operates its own multi-region redundancy. SendTax inherits Clerk's availability for sign-in flows.

6.6 Operational resilience

- **Infrastructure as code:** Fly configurations are committed to the monorepo (`fly.api.prod.toml`, `fly.worker.prod.toml`, and the per-app `fly.toml` files). The cluster can be re-provisioned from version control.
- **Secrets recovery:** Application secrets are stored both in Fly encrypted secrets and (operator-accessible) in environment-scoped 1Password vaults, so the loss of either does not prevent rebuilding the cluster.
- **1Password Emergency Kit** is maintained for both co-founders, providing recovery access to all credentials in the event one co-founder is unavailable.

7. Single points of failure

SendTax enumerates these rather than hide them.

SPoF	Risk	Current mitigation
Fly.io region iad	A region-wide Fly outage takes down all SendTax application services simultaneously	Reactive: rebuild in an alternate Fly region from infrastructure-as-code and managed-Postgres restore if `iad` is unrecoverable for an extended period
Celery Beat scheduler	Exactly one Beat instance runs; periodic tasks (training-purge sweep, scheduled obligations, reminders) stop if it crashes and auto-restart fails	`[[restart]] policy = "always"` auto-restarts Beat with up to 5 retries. Beat crashes affect scheduling, not customer-facing reads. A watchdog alert is on the near-term roadmap to detect cases where auto-restart does not recover Beat (§11).
Single application database cluster	Database corruption — not just outage — would affect the live database	Daily backups + PITR per §6.2; backups are managed-service-encrypted and stored by Fly

Cloudflare R2 bucket	A bucket-level configuration error or compromised credential could affect document availability	Application-layer encryption means a compromised bucket does not expose document plaintext. Object versioning on the documents bucket protects against application-bug-induced deletion (§6.3).
GCP KMS key version availability	If a KEK version becomes unavailable (deletion, account compromise, GCP outage), documents wrapped under that version cannot be decrypted until access is restored	Dual-key support allows rotation without losing access to previously-wrapped DEKs. SendTax does not currently destroy KEK versions as a routine disposal mechanism.
Key-person availability	A two-person operating team is sensitive to individual unavailability during an incident	Both operators have full administrative access to most systems; production deploy access is currently held by Liam Howell only. Break-glass production deploy access for Holly Gibbs is on the near-term roadmap. An external operator on retainer for true business-continuity coverage is on the near-term roadmap (§11).

8. Threat scenarios and recovery procedures

Procedures are organized by failure scope. Each procedure is the intended action; the **Incident Response Policy** governs the broader response (declaration, communication, postmortem).

8.1 Single machine failure

- **Scope:** One Fly machine fails (process crash, VM death).
- **Detection:** Fly health checks fail; Sentry may surface symptoms.
- **Procedure:** Fly auto-restarts the machine. No operator action is required in most cases. If auto-restart loops, the on-call operator investigates and may roll back the most recent deployment.

- **Expected recovery:** Seconds to minutes.

8.2 Application deployment failure

- **Scope:** A bad deploy makes the API or worker unhealthy.
- **Detection:** Failed health checks block deployment; Sentry surfaces errors post-deploy if a subtle regression slips through.
- **Procedure:** Roll back to the previous image tag (`fly deploy --image <previous-tag>`). Investigate after rollback; do not debug in production.
- **Expected recovery:** Minutes.

8.3 Database outage (within Fly.io managed service)

- **Scope:** Managed Postgres becomes unavailable but the cluster is still under Fly's control.
- **Detection:** API health checks fail with database errors; Sentry surfaces connection failures.
- **Procedure:** Engage Fly.io support immediately. Fly's managed service is responsible for failover; SendTax monitors and communicates.
- **Expected recovery:** Per Fly Managed Postgres SLA.

8.4 Data corruption requiring restore

- **Scope:** Logical corruption (a bad migration, application bug writing wrong data) where the live database is intact but contains incorrect data.
- **Procedure:**
    1. Stop write-path workers immediately (`fly scale count 0` on `st-worker-prod`)
    2. Determine the corruption window (when did the bad writes begin?)
    3. Engage Fly support to restore from PITR to the latest pre-corruption point
    4. Reconcile any legitimate writes that occurred in the corruption window (the corruption window will lose those — that is the RPO trade-off)
    5. Resume workers
- **Expected recovery:** Hours, dominated by the PITR restore and the reconciliation.

8.5 Region-wide Fly.io outage

- **Scope:** Fly.io's `iad` region is down for an extended period.
- **Procedure:**
  - Declare a Critical incident per the **Incident Response Policy**
  - Monitor Fly's status page while preparing a regional rebuild. Most regional outages resolve in hours; rebuild adds risk and is the slower path
  - If the outage exceeds the threshold at which Fly indicates sustained unrecoverability, rebuild the application in an alternate Fly region using the committed `fly.toml` configs. This requires:
    - Provisioning a new Managed Postgres cluster in the new region and restoring from the latest available backup
    - Re-creating Fly secrets in the new apps from 1Password vaults
    - Updating DNS to point to the new region
  - Customer notification follows the incident-response timeline
- **Expected recovery:** Hours for the first option; a day or more for a full region rebuild. This procedure has not been rehearsed (§11).

8.6 Cloudflare R2 outage

- **Scope:** R2 is unavailable; uploads and downloads of customer documents fail.
- **Procedure:** Customer document operations degrade gracefully — the UI surfaces "temporarily unavailable" messages and queues operations where safe. The database remains writable, so non-document operations (intake, profile changes, return progress) continue. SendTax waits for R2 recovery; no manual restore is meaningful.
- **Expected recovery:** Per Cloudflare's published terms.

8.7 GCP KMS outage

- **Scope:** KMS unwrap calls fail.
- **Procedure:** Document decryption fails. The UI surfaces the condition. The database remains accessible for non-document operations. SendTax waits for GCP recovery.
- **Expected recovery:** Per Google Cloud KMS SLA.

8.8 Clerk outage

- **Scope:** Customers cannot sign in; existing sessions continue until their tokens expire.
- **Procedure:** Engage Clerk support; surface degraded sign-in to customers. The data remains intact behind authentication; no manual recovery is meaningful.
- **Expected recovery:** Per Clerk's published terms.

8.9 Loss of an operator device

- **Scope:** A SendTax operator's laptop is lost, stolen, or compromised.
- **Procedure:**
    1. Revoke the operator's GitHub, Fly.io, Clerk, GCP, Cloudflare, Postmark, Sentry, PostHog, Modal, and 1Password sessions
    2. Rotate any secrets to which the operator had unique access
    3. Verify the device's full-disk encryption was active at the time of loss; if not, treat as a potential data-access incident under the **Incident Response Policy**
    4. Re-issue access from a known-clean device

8.10 Key-person unavailability

- **Scope:** One of two operators is unavailable during an incident.
- **Procedure:** The remaining operator has full administrative access to most systems. Internal runbooks for the most common recovery scenarios are maintained at `st-apps/docs/RUNBOOKS.md` *(verified path 2026-05-26; the expanded runbook covering deploy, rollback, secret rotation, every BCP §8 scenario, and observability checks is being ported into the repo from the "Runbooks.md expansion" working document)*. For production deploy access during Liam's unavailability, see the break-glass procedure (§9.3, currently on roadmap). For extended unavailability of both operators, see the external operator on retainer (§11).

9. Roles and personnel availability

9.1 Roles during recovery

Recovery roles map onto the incident-response roles described in the **Incident Response Policy** §5:

- **Incident Commander** — declares the recovery event, assigns severity, drives the timeline, decides when to declare recovery complete
- **Technical Lead** — executes the technical recovery work (restoration, redeploy, verification)
- **Communications Lead** — drafts customer notifications and external statements

In a two-operator team, one person may hold multiple roles during a small incident. For Critical incidents, the Incident Commander and Communications Lead must be different people whenever both operators are available.

9.2 Current personnel posture

SendTax is currently operated by two co-founders (Holly Gibbs and Liam Howell). Several operational responsibilities are currently held by a single person:

- **Production deploy access** is restricted to Liam Howell (see **Access Control Policy** §5.3)
- **Admin dashboard access** is held by both co-founders

The single-deploy-access posture reflects deliberate single-owner accountability for production changes during this stage. The associated availability risk is named explicitly in §7 and addressed by the measures below.

9.3 Break-glass production deploy access

A break-glass production deploy capability is being established for Holly Gibbs, to be used only in the event of Liam Howell's unavailability during a recovery event. The credential is stored such that:

- It is not used in normal operation
- Its use is recorded and audited
- It is rotated immediately upon use

- It is reviewed at each access review (per **Access Control Policy** §5.5)

Implementation of break-glass deploy access is on SendTax's near-term roadmap (§11).

9.4 Succession beyond unavailability

The scenario of permanent unavailability of a co-founder (departure, incapacity, death) is partially addressed by the access measures above. A more complete succession plan, including legal and operational continuity decisions, is on SendTax's longer-term roadmap.

10. Backup integrity and RTO/RPO

10.1 Backup creation and verification

- **Backup creation** is performed by Fly.io Managed Postgres. SendTax does not produce parallel backups.
- **Backup encryption at rest** is provided by the managed service.
- **Restore verification** — confirming that backups actually restore to a working database — has not yet been formally rehearsed by SendTax. The first DR test is scheduled within six months of policy publication (§11).

10.2 RTO and RPO targets

SendTax does **not** currently publish formal RTO or RPO targets.

Any RTO or RPO published today would be derived from provider SLAs rather than measured from a tested recovery procedure. SendTax prefers to publish nothing rather than publish a target that cannot be defended.

What can be described candidly:

- **Effective RPO** is bounded by the Managed Postgres PITR window for the database, and by R2's published durability for the document store
- **Effective RTO** depends on the scenario. Single-machine failures recover in seconds; a region rebuild has not been rehearsed and SendTax will not state a number until it has

Formal RTO and RPO targets will be published after the first scheduled DR test completes (§11).

11. Roadmap commitments

The following commitments are not currently in production. Each is listed here with the gap and the indicative timeline. Once each commitment is implemented, this policy will be revised to reflect current state and the corresponding line removed.

Commitment	Current state	Gap	Target
First DR test (restore drill)	Not yet conducted	Schedule, execute, document	Within six months of policy publication
DR test cadence increase to semi-annual	Cadence: annual until first test completes	Increase cadence after first successful test	After first DR test
Formal RTO/RPO targets	Not formally defined	DR test must complete first	After first DR test
Break-glass production deploy access for Holly	Liam is sole holder of production deploy access	1Password Emergency Kit pattern or equivalent	Within 30 days of policy publication
Celery Beat watchdog alert	Auto-restart configured; no alert when retries are exhausted	Heartbeat-based alert (Sentry monitor, Better Stack, or similar)	Within 30 days of policy publication
Public status page	No dedicated page; current channel is email + incident-system fan-out	Vendor selection or build decision pending Liam's input	Decision pending tomorrow's discussion

External operator on retainer	No external operator	Vendor selection and onboarding	Within 6 months of policy publication
Regional rebuild drill	Not yet conducted	Documented and tabletop-tested rebuild in alternate Fly region	Longer-term — after first DR test
Cross-provider failure playbook	Not documented	Compounded-failure scenarios not playbooked	Longer-term
Co-founder succession plan beyond temporary unavailability	Partial via 1Password Emergency Kit	Legal and operational continuity not formalized	Longer-term

12. Testing

The components of this plan are exercised in the following ways:

- **Production health checks** continuously verify single-machine resilience
- **Routine deployments** rehearse the rollback procedure roughly weekly
- **Tabletop exercises** for representative scenarios (regional outage, data corruption, key-person unavailability) — first scheduled within six months per the **Incident Response Policy** §15
- **DR test (restore drill)** — annual cadence, increasing to semi-annual after the first successful test completes (§11). What a DR test covers:
    - Restoring a recent production database snapshot or PITR target to a staging environment
    - Verifying data integrity against an expected baseline
    - Documenting the time elapsed from restore-trigger to verified-restored
    - Documenting any gaps, surprises, or runbook errors
    - Updating the runbook and this policy if the test reveals capabilities different from those described

Test records (date, scope, findings, corrective actions, named participants) are retained internally and made available to auditors on request.

13. Communication during disruption

13.1 Internal communication

During a declared recovery event, internal communication follows the **Incident Response Policy** §7.5. The Incident Commander coordinates; the Scribe maintains the timeline.

13.2 Customer communication

Customers are notified through the same audited fan-out infrastructure documented in the **Incident Response Policy** §9. Initial notifications go out as soon as SendTax has a defensible factual picture; updates are sent as the picture develops, rather than waiting for full recovery.

For events affecting authentication or document availability, all customers are notified. For events affecting only filers or only firms, notification is scoped accordingly. A public status page is on the roadmap (§11); in the interim, customers are notified directly during incidents.

13.3 Sub-processor communication

When a recovery event involves a sub-processor, SendTax follows the **Vendor Management Policy** §11 and the **Incident Response Policy** §13: engaging the provider's published channel, tracking provider communications on SendTax's incident timeline, and notifying customers based on the full picture rather than just SendTax's actions.

14. Continuous improvement

This plan is updated when any of the following occurs:

- A real incident reveals a gap
- A sub-processor changes its published availability terms
- A new component is introduced that changes the BIA in §5
- A roadmap item from §11 ships and graduates into a measured commitment

Each update is recorded in the version line at the top of this document.

15. Exceptions

Any deviation from this policy — for example, declining to execute a documented recovery procedure because of an unusual circumstance — requires:

1. Approval from a second SendTax operator (or, if only one is available, retrospective documentation reviewed at the next access review)
2. A documented justification recorded on the incident timeline
3. A defined re-evaluation point

Exceptions are reviewed at each policy review and in any post-incident postmortem.

16. Enforcement

Violations of this policy may result in revocation of access, termination of employment or contract, and, where applicable, civil or criminal referral.

17. Related policies

- **Information Security Policy** — umbrella policy
- **Incident Response Policy** — shared roles, notification system, severity levels
- **Access Control Policy** — break-glass access controls; production deploy access model
- **Encryption Policy** — KEK durability; cryptographic disposal mechanics; dual-key migration
- **Data Retention & Disposal Policy** — backup retention; data lifecycle
- **Vendor Management Policy** — sub-processor recovery dependencies

18. Document control

Version	Date	Author	Notes
1.0	May 21, 2026	Holly Gibbs	Initial publication

19. Contact

Incident reporting	security@send.tax

Service status	Customers are notified directly during incidents. A public status page is on the roadmap.
Privacy inquiries	privacy@send.tax
Operating entity	Howell & Gibbs LLC (operator of SendTax)