SendTax

TRUST CENTER

Incident Response Policy

Cryptographic standards, algorithms, and key-management practices.

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 incident-response systems or regulatory obligations

---

1. Purpose

This policy describes how SendTax detects, contains, communicates about, and learns from security incidents. It supports the commitments made in the **Information Security Policy** and aligns with SOC 2 Common Criteria CC7.3 and CC7.4.

2. Scope

This policy covers any event that:

- Compromises (or is reasonably suspected to compromise) the confidentiality, integrity, or availability of customer data
- Compromises (or is reasonably suspected to compromise) the authentication or authorization controls protecting that data
- Causes a sustained outage of SendTax services that affects customers' ability to access or file their data
- Is reported to SendTax by a customer, researcher, employee, or sub-processor and meets any of the above descriptions

Lower-severity operational issues (an individual user's bug, a transient deploy hiccup) follow our internal operations runbooks and are not the subject of this policy.

3. Definitions

Term	Meaning
Event	Any observable occurrence in a SendTax system. Most events are routine.
Incident	An event, or a chain of events, that meets the scope criteria above.
Declared incident	An incident that has been formally opened in our internal Security Incident system with an assigned severity, owner, and tracking ID.
Breach	A subset of incidents in which personal data was actually (not just potentially) accessed or exfiltrated by an unauthorized party. Breaches trigger regulatory notification obligations (see §10).
Postmortem	Written analysis published after resolution of an incident, covering what happened, why, what we did, and what we are changing.

4. Severity classification

Every declared incident is assigned one of four severity levels. The severity controls response urgency, notification timing, and who must be engaged.

Severity	Definition	Examples
Critical	Confirmed unauthorized access to customer data, confirmed data exfiltration, complete outage of authentication, or any incident requiring same-day regulatory notification.	Database compromise; KMS key exposure; total auth-provider outage; ransomware against production.
High	Strong evidence of attempted compromise affecting multiple customers, or sustained partial outage of a core service.	Credential-stuffing wave breaching rate limits; widespread document-decryption failures; outage of document upload for >30 minutes.

Medium	Isolated compromise of a single non-admin account; security-relevant misconfiguration discovered in production; vulnerability disclosure requiring an urgent patch.	One filer's account taken over via reused password; an internal-only endpoint accidentally made public; a high-severity dependency CVE.
Low	Security-relevant event that warrants tracking but does not threaten customer data.	Anomalous error spike traced to a benign cause; reconnaissance traffic blocked by rate limiting; non-exploitable misconfiguration.

Severity is initially assessed by the Incident Commander on declaration and may be raised or lowered as the picture clarifies. Severity changes are themselves logged as updates on the incident timeline.

5. Roles and responsibilities

SendTax is a small organization. Incident-response roles are assigned per-incident rather than to fixed individuals; any administrator may fill any role, and a single person may hold multiple roles during a small incident.

Role	Responsibilities
Incident Commander	Single decision-maker for the incident. Declares the incident, assigns severity, drives the response timeline, decides when to resolve.
Technical Lead	Owns containment and remediation work. May or may not be the same person as the Commander.
Communications Lead	Drafts customer notifications and external statements. Must approve any communication that leaves the company.
Scribe	Maintains the incident timeline by posting updates as the situation evolves. Often the Incident Commander on a small team.

For Critical-severity incidents, the Incident Commander and Communications Lead must be different people whenever there are at least two operators available.

6. Detection

SendTax detects incidents through a combination of automated monitoring and human reports.

6.1 Automated detection

- **Application errors and anomalies** are captured by Sentry across backend, worker, and frontend deployments.
- **Authentication anomalies** (failed login spikes, suspicious sign-in patterns) are surfaced by Clerk and supplemented by SendTax application logs.
- **Infrastructure health** is monitored via Fly.io's platform metrics and SendTax's `/healthz` and `/readyz` endpoints.
- **Audit-log anomalies** can be queried against the hardened `audit_log` table for forensic investigation.

6.2 Human reports

- **External security researchers** may report vulnerabilities to **security@send.tax**. See §14 for SendTax's responsible disclosure commitments.
- **Customers** may report security concerns through any support channel; reports are escalated to the Incident Commander on duty.
- **Employees** are expected to report any security-relevant observation immediately, with no penalty for reporting events that turn out to be benign.

7. Response process

Once an incident is declared, response follows six phases. Phases may overlap; a complex incident may revisit earlier phases as new information emerges.

7.1 Declare

The Incident Commander creates a record in the Security Incident system with:

- A unique slug and human-readable title
- An initial severity assessment
- An internal summary of what is known and unknown

- A start time (when the underlying issue began, to the best of current knowledge — not when it was detected)

The record opens in `investigating` status.

7.2 Contain

Containment work is prioritized over root-cause analysis. Standard containment actions, applied as appropriate to the incident:

- Revoke compromised credentials (Clerk, Google Cloud KMS, Fly.io, GitHub)
- Rotate any potentially exposed secrets (JWT signing keys, API tokens, database credentials), following the documented secret-rotation runbook
- Suspend affected accounts or tenant-filer links
- Block known-bad IPs or user-agent patterns at the application or edge layer
- If necessary, take a service offline rather than continue serving compromised data

7.3 Eradicate

Eradication identifies and removes the underlying cause:

- Patch the vulnerability in code, configuration, or infrastructure
- Remove any persistence mechanisms (unauthorized accounts, schedules, cron entries, OAuth grants)
- Verify that the exploit path no longer functions

7.4 Recover

- Restore affected services to normal operation
- Restore any deleted or corrupted data from backups where applicable
- Re-enable any features or accounts that were suspended for containment
- Move the incident to `monitoring` status and watch for recurrence

7.5 Communicate

Communications are issued in parallel with — not after — the technical response, beginning as soon as we have a defensible factual picture. See §9 for customer-notification policy.

7.6 Close and learn

When the Incident Commander is satisfied the incident is fully resolved, they:

- Set the status to `resolved` and record a resolution timestamp
- Schedule a postmortem (mandatory for Critical and High; recommended for Medium; optional for Low)
- Capture corrective actions in the team backlog with named owners and target dates

8. Incident lifecycle

SendTax tracks declared incidents through four explicit statuses, enforced as a database constraint in the Security Incident system:

1. **`investigating`** — incident declared; cause and scope are being established
2. **`identified`** — root cause and affected scope are understood; remediation work is underway
3. **`monitoring`** — fix has been applied; SendTax is watching for recurrence or downstream effects before declaring resolution
4. **`resolved`** — incident is closed. A timestamp is recorded and postmortem work (if required) begins

Movement between statuses is recorded as an append-only update on the incident's timeline.

9. Customer notification

SendTax has a built-in mechanism for communicating with customers during incidents. Notifications are issued from the Security Incident system itself, which guarantees that:

- Each communication is tied to a specific incident record
- Each recipient is mailed at most once per notification, even on retried delivery (idempotency enforced at the database level)
- The notification fan-out is auditable: every queued, sent, failed, and skipped delivery is recorded

9.1 Audiences

Notifications can be targeted at:

- **All customers** (filers + tax professionals) — used when the incident affects everyone or when audience scoping is not yet certain
- **Filers only** — used when the incident affects only individual taxpayer accounts
- **Pros only** — used when the incident affects only firms and their staff

9.2 Templates and timing

SendTax commits to notifying affected customers **without undue delay, and in any event within 72 hours of confirming that an incident materially affects their data**. This commitment applies in addition to any shorter notification timeline required by law or contract (see §10).

Template	Sent when	Contents
Initial	Within 24 hours of declaration for Critical/High; promptly after declaration for Medium; at the Commander's discretion for Low.	What we observed, what we don't yet know, what customers should do (if anything), where to get updates.
Update	Whenever a material development occurs (containment achieved, scope clarified, fix deployed).	New information; corrections to previously-stated facts; revised expected timeline.
Resolved	Once the incident is `resolved` and a public summary is ready.	What happened, what we did, what we are changing, link to postmortem when published.

9.3 Tone and accuracy

- Initial communications **do not speculate** about cause or scope. They state what we observed and acknowledge what we do not yet know.
- We **do not minimize**. If we are unsure whether data was accessed, we say so plainly rather than implying it was not.

- We **correct ourselves in writing** when later facts contradict earlier statements, via a follow-up notification rather than by editing prior ones. The incident timeline is append-only by design.

10. Regulatory and contractual obligations

For incidents involving personal data, SendTax notifies regulators and affected individuals on the timelines required by applicable law, including:

- **FTC Safeguards Rule (16 CFR Part 314.5):** notification to the FTC within **30 days** of discovering a security event involving the unauthorized acquisition of unencrypted customer information of 500 or more consumers.
- **IRS and tax-data regulations:** notification to the IRS and applicable state tax agencies consistent with SendTax's obligations as a handler of taxpayer data under federal and state tax-privacy statutes, including notification expectations articulated in IRS Publication 4557 for tax-data handlers.
- **U.S. state breach notification laws:** notification on the most stringent timeline applicable to affected individuals' states of residence. Several states (including California, Colorado, Florida, and New York) impose specific timing or content requirements.
- **GDPR (Article 33–34):** notification to the relevant supervisory authority within **72 hours** of becoming aware of a personal-data breach affecting EU/UK data subjects, and direct notification to affected individuals when the breach is likely to result in high risk to their rights and freedoms.
- **Contractual commitments to customers:** any shorter-than-statutory notification timeline agreed in a Data Processing Agreement or master services agreement takes precedence over the timelines in this policy.

The Communications Lead is responsible for confirming which notification obligations apply to a given incident and for ensuring each one is met.

11. Internal record-keeping

Every declared incident produces a durable internal record:

- **The incident row** — title, severity, status, start, resolution, internal summary, public summary

- **The append-only timeline** — every status change, every update, every notification. Updates are not edited or deleted in normal flow; corrections are posted as follow-up updates.
- **Notification audit** — every email blast and every per-recipient delivery, retained for compliance review

This record is the source of truth for any later investigation, audit, or regulatory inquiry. Retention follows the **Data Retention & Disposal Policy**.

12. Postmortems

Postmortems are mandatory for Critical and High incidents, recommended for Medium, and optional for Low. They are completed within **10 business days** of resolution.

Each postmortem covers:

- **Summary** — one paragraph anyone in the company can understand
- **Timeline** — derived from the incident's append-only updates plus any additional reconstruction from logs
- **Root cause** — including any contributing factors (process, staffing, tooling)
- **Detection** — how we found out, how long the gap was between start and detection
- **Response** — what we did, what worked, what did not
- **Impact** — concrete numbers (customers affected, data records touched, downtime duration, financial impact if known)
- **Corrective actions** — concrete items with named owners and target dates. These flow into the team backlog and are tracked to completion.

Postmortems are blameless: they describe how the system failed, not who failed.

12.1 Public postmortems

For incidents that materially affected customers, a customer-facing postmortem summary is published as the final notification on the incident record. Public postmortems describe what happened, what we did, and what we are changing — without disclosing details that would help future attackers (e.g., the specific exploit path of a fixed vulnerability).

13. Coordination with sub-processors

When an incident originates with or is exacerbated by a sub-processor (Clerk, Fly.io, Google Cloud, Cloudflare, Resend, Sentry, Modal), SendTax:

- Engages the provider's published incident-response or support channel immediately
- Tracks the provider's communications on SendTax's own incident timeline so customer notifications reflect the full picture
- References the provider's published incident postmortem (where available) in SendTax's own postmortem

SendTax is responsible for notifying its customers regardless of whether the underlying issue was within SendTax-operated infrastructure or a sub-processor's.

14. Reporting a security concern

SendTax welcomes reports of security vulnerabilities, suspected breaches, or concerning observations.

Channel	Use for
security@send.tax	Vulnerability disclosures, suspected breaches, anything time-sensitive
privacy@send.tax	Privacy-specific concerns and data subject requests

SendTax commits to:

- Acknowledging reports sent to **security@send.tax** within **2 business days**
- Working in good faith with researchers who follow responsible disclosure practices
- Not pursuing legal action against researchers acting in good faith under recognized safe-harbor norms (CFAA carve-outs for authorized testing and equivalent provisions in other jurisdictions)

15. Testing

- This policy and the underlying response infrastructure are reviewed at least **semi-annually**.
- **Tabletop exercises** — walkthrough simulations of representative incidents to validate the response process and team familiarity — are conducted at least **annually**. *(2026-05-26 schedule: the first annual tabletop is targeted for 2026-09-15, comfortably within the six-month window from policy publication. The scenario will be selected from BCP §8 — likely §8.4 "data corruption requiring restore", since it exercises the database-recovery runbook + customer-notification fan-out + corruption-window write reconciliation in a single drill.)*
- Components of the response system (notification fan-out, audit-log writes, status transitions) are covered by automated tests in SendTax's CI pipeline.

16. Exceptions

Any deviation from this policy — for example, a deliberate delay in customer notification at the request of law enforcement — requires:

1. Approval from a second SendTax operator
2. A documented justification recorded on the incident timeline
3. A defined re-evaluation point

Exceptions are reviewed in the post-incident postmortem and at the next policy review.

17. Enforcement

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

18. Related policies

- **Information Security Policy** — umbrella policy that this document supports
- **Access Control Policy** — controls referenced during containment and credential rotation

- **Encryption Policy** — key-compromise response and cryptographic erasure
- **Data Retention & Disposal Policy** — retention of incident records and notifications
- **Vendor Management Policy** — sub-processor obligations during incidents

19. Document control

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

20. Contact

Security disclosures	security@send.tax
Privacy inquiries	privacy@send.tax
Operating entity	Howell & Gibbs LLC (operator of SendTax)