SendTax

TRUST CENTER

Vendor Management Policy

How third-party vendors and sub-processors are selected, monitored, and removed.

Effective: May 21, 2026 Owner: Howell & Gibbs LLC Status: v1 – initial publication

Review cadence: Semi-annual, or after any material change to vendor relationships or regulatory obligations

---

1. Purpose

This policy defines how SendTax selects, evaluates, contracts with, monitors, and offboards third-party vendors that process or have access to customer data, or that operate infrastructure on which SendTax depends. It supports the commitments made in the **Information Security Policy** and aligns with:

- **SOC 2 Common Criteria CC9.1 and CC9.2** — third-party risk management
- **FTC Safeguards Rule §314.4(f)** — service provider oversight requirements for financial institutions
- **IRC §7216** — federal restrictions on the disclosure of tax return information to vendors

SendTax is a "financial institution" under the Gramm-Leach-Bliley Act because it handles taxpayer financial information. Vendor oversight is therefore a legal obligation, not solely a security best practice.

2. Scope

This policy applies to all third parties that process, store, transmit, or have potential access to SendTax customer data or production systems, including:

- **Sub-processors** — vendors that process customer data on SendTax's behalf

- **Operational vendors** — vendors that support SendTax operations without normally processing customer data
- **Internal-only tools** — vendors used by SendTax personnel that never touch customer data
- **Contractors and consultants** with access to SendTax systems (governed in combination with the **Access Control Policy**)

3. Principles

- **Customer trust is non-transferable.** When a vendor handles customer data on SendTax's behalf, the customer's trust still sits with SendTax. SendTax is responsible for vendor behavior with respect to customer data.
- **Necessity before convenience.** Every vendor relationship begins with a question: is this service necessary, or are we adding surface area for ergonomic reasons? Vendor count is treated as a cost.
- **U.S. data residency by default.** Customer data is processed by U.S.-based providers in U.S. regions. SendTax operates U.S.-only; non-U.S. processing of tax return information would require IRC §7216-compliant consent that SendTax does not currently use.
- **Defense in depth across the supply chain.** No single vendor's compromise should be sufficient to expose customer data; SendTax's own encryption and access controls remain in place even when a vendor is involved.
- **Risk-proportional diligence.** Diligence depth scales with vendor tier; SendTax does not apply enterprise-grade processes to vendors handling no customer data.
- **Transparent to customers.** The current sub-processor list is published, and material changes are communicated in advance.

4. Definitions

Term	Meaning
Vendor	Any third party that provides a service to SendTax. Includes both sub-processors and internal-only tools.
Sub-processor	A vendor that processes, stores, or transmits personal data on SendTax's behalf in the course of delivering SendTax's services.

DPA	Data Processing Agreement (or Addendum). The contractual instrument that documents how a sub-processor will handle personal data and what their obligations are.
Personal data	Any information relating to an identified or identifiable individual, including taxpayer data, identity documents, contact information, authentication data, and behavioral telemetry tied to identified users.

5. Vendor tiers

Every vendor is classified into one of three tiers at onboarding. The tier determines diligence depth, contractual requirements, monitoring cadence, and whether changes require customer notification.

5.1 Tier 1 — Customer-data sub-processors

Definition. The vendor processes, stores, or transmits identifiable customer personal data — including tax-return data, identity documents, contact information, authentication data, or behavioral telemetry tied to identified users.

Examples in current use: Fly.io (hosting + database), Cloudflare R2 (document storage), Clerk (identity), Google Cloud KMS (key management), Postmark (transactional and inbound email — including taxpayer documents arriving via email; Resend cutover Phase 1 shipped behind the `INBOUND_BACKEND` feature flag per PR #69), Modal (ML inference), Sentry (error monitoring), PostHog (product analytics — session recording disabled at the SDK level via `disable_session_recording: true`; outbound events sanitized through a PII denylist at `before_send`; surveys and dead-click capture disabled — see `st-apps/packages/analytics/src/posthog.ts`), Stripe (payments).

(Microsoft Clarity was removed from the SendTax stack on 2026-05-26 per PR #67 and is no longer a sub-processor. The Content Security Policy still allowlists `*.[clarity.ms](<http://clarity.ms>)` from an earlier deploy and is being cleaned up in Phase 2.)

Onboarding requirements:

- Signed Data Processing Agreement (DPA)

- Documented data flows: what personal data category goes to the vendor, why, and how it returns or is destroyed
- Review of the vendor's most recent independent security attestation (SOC 2 Type II preferred, ISO 27001 or equivalent acceptable) — or onboarding under the §5.4 exception path
- Confirmation of U.S. data residency
- For vendors processing tax return information: §7216 auxiliary-service notice and contractual restriction to allowed auxiliary services
- Listing on the public Sub-Processor List **before** production cutover

Ongoing requirements:

- Annual review of the vendor's published security posture and attestation renewal
- Inclusion in the internal vendor inventory with data categories tracked
- Material changes (vendor replacement, new data category, change of data residency) trigger customer notification per §9

5.2 Tier 2 — Operational vendors with incidental customer-data exposure

Definition. Vendors that in normal operation do not handle identified customer personal data, but could see limited customer data in operator-driven workflows (e.g., debugging sessions, support escalations).

Examples in current use: GitHub (source control — must never contain customer data; checked via automated secret-scanning).

Onboarding requirements:

- DPA where the vendor provides one as a standard offering
- Confirmation that customer personal data is not deliberately written to the vendor
- Internal access controls limiting which operators can pull customer data into the vendor's surface

Ongoing requirements:

- Reviewed biennially or on material event
- Listed in the internal vendor inventory (not on the customer-facing Sub-Processor List)

5.3 Tier 3 — Internal-only tools

Definition. Vendors used by SendTax personnel that have no exposure to customer personal data in any mode of operation.

Examples in current use: 1Password (operator credentials), domain registrar, design and productivity tools.

Onboarding requirements: Standard vendor terms-of-service acceptance. No formal DPA required.

Ongoing requirements: No active monitoring beyond normal account hygiene; covered at the annual vendor review by inventory verification only.

5.4 Defined exception path for Tier 1 attestation gap

A Tier 1 vendor that does not hold a current direct SOC 2 Type II report (or equivalent attestation in its own name) may be onboarded or retained only if all of the following conditions are met:

1. The vendor's parent company or operating entity holds a current SOC 2 Type II report whose scope demonstrably covers the vendor's product and systems, and SendTax has obtained or reviewed that report
2. Documented compensating controls are in place to mitigate the attestation gap
3. The exception is approved by **both co-founders** (rather than a single operator)
4. The vendor is reviewed annually, with the exception re-evaluated at each review and removed once the vendor obtains direct attestation or is replaced

The exception path exists for cases where a strong sub-processor (e.g., a vendor whose parent has SOC 2 with adequate scope) cannot supply a direct attestation in its own name. It is not a workaround for vendors with no current attestation at all.

6. Selection criteria

When evaluating a candidate vendor, SendTax considers:

Criterion	What SendTax looks for

Security posture	Independent attestations (SOC 2 Type II preferred); published security program; credible disclosure history
Data residency	U.S. regions available and configurable as default
Encryption	TLS in transit; AES-256 at rest; KMS-backed key custody where applicable
Access controls	SSO support; role-based access; audit logs available to SendTax as customer
Sub-processor transparency	Vendor publishes its own sub-processor list and notifies of changes
DPA quality	Clear breach-notification timeline; clear sub-processor flow-down; clear deletion-on-termination commitment
Financial stability and longevity	Credible runway; stable customer base or open-source fallback
Exit path	Reasonable data export; ability to migrate without re-engineering
Cost	Considered last, after security and fit

7. Contractual requirements

7.1 What a DPA must address

Each Tier 1 sub-processor relationship is governed by a written DPA (or equivalent contract clause). The DPA must address, at minimum:

- The categories of personal data processed and the purposes of processing
- The vendor's obligation to process personal data only on documented instructions from SendTax
- Confidentiality commitments for the vendor's personnel
- The vendor's technical and organizational security measures
- The vendor's obligation to notify SendTax of any personal-data breach without undue delay, supporting the timelines in the **Incident Response Policy** §10

- The vendor's use of further sub-processors, including SendTax's ability to object
- The vendor's obligation to assist SendTax with data-subject requests and breach notification
- Deletion or return of personal data on termination of the relationship
- Audit rights — typically satisfied by the vendor's independent attestation reports rather than on-site audits

7.2 IRC §7216 obligations

Vendors that process **tax return information** (as defined in IRC §7216) must:

- Receive the §7216 auxiliary-service notice required for tax-return preparers' agents
- Be contractually restricted to allowed auxiliary services
- Be U.S.-based, or, if non-U.S., subject to specific §7216-compliant consent (a path SendTax does not currently use)

7.3 Current DPA status

(2026-05-26 status: DPA collection is in progress across the 10 Tier 1 sub-processors. Holly is leading the chase; Liam reviews technical clauses. The current state — signed / draft / requested — is tracked in the internal vendor inventory and reported at each semi-annual policy review. Where a DPA is not yet in place, the relationship is operating under the vendor's standard terms-of-service and is documented as an exception under §14 with a defined re-evaluation point. The full DPA matrix will be made available to enterprise customers on request.)

8. Onboarding process

For a Tier 1 vendor, the onboarding process is:

1. **Need check.** Document the specific job the vendor will do and confirm no existing vendor already covers it.
2. **Candidate evaluation.** Apply §6 criteria to a short list of candidates.
3. **Security and contractual review.** Pull the vendor's SOC 2 or equivalent; review the DPA against §7.1 requirements; negotiate changes where necessary.

4. **Data-flow mapping.** Document what personal-data categories will leave SendTax, in what form (plaintext, encrypted-by-SendTax, etc.), and how they return.
5. **Integration with security baseline.** Configure access controls, audit logging, and secret storage per **Information Security Policy** and **Access Control Policy**.
6. **Sub-Processor List update.** Add the vendor to the public Sub-Processor List **before** any production data flows.
7. **Customer notification.** Material new vendors (touching new data categories) trigger advance notification per §9.
8. **Cutover.** Production traffic begins.

For Tier 2 and Tier 3 vendors, onboarding is documented in the internal vendor inventory but does not require the full checklist above.

9. Sub-Processor List and customer notification

SendTax maintains a public Sub-Processor List that identifies every Tier 1 sub-processor. The list is the customer-facing artifact of this policy and is the canonical source of truth.

The Sub-Processor List records, for each entry:

- Vendor legal name and URL of their security/trust page
- The service the vendor provides to SendTax
- The category of personal data the vendor may process
- The processing region
- The vendor's current independent attestations
- Date of most recent SendTax diligence review
- A link to the vendor's published DPA or sub-processor list

The current list is published at [link to Sub-Processor List page].

9.1 Notification of changes

SendTax notifies customers of additions, removals, or material changes to the Sub-Processor List by:

- **Publishing the change on the Sub-Processor List page** as the canonical record

- **Posting an entry in a change-digest accessible from that page**, which customers may opt to receive by email

There is no automatic individual-email push for every change. Material changes take effect no fewer than **30 days** after publication on the Sub-Processor List page, providing customers an opportunity to review and raise concerns through privacy@send.tax.

For incident-driven changes (e.g., emergency removal of a compromised vendor), SendTax may make the change effective immediately and publish the rationale promptly thereafter.

Customers who object to a new sub-processor may contact SendTax at privacy@send.tax. SendTax will work with the customer to identify a mutually acceptable path; if no acceptable path is available, the customer may terminate their use of the affected service.

10. Ongoing monitoring

Tier	Cadence	What is reviewed
Tier 1	Annual	Current attestation report; sub-processor list changes; incident history; any material change in vendor ownership, jurisdiction, or scope
Tier 2	Biennial	Same scope as Tier 1 but lower frequency
Tier 3	Event-driven	Reviewed on incident, change in scope, or change in vendor ownership

Findings are documented. A material adverse change in a vendor's posture may trigger reclassification, additional diligence, or replacement.

10.1 What SendTax does not do

- SendTax does not conduct on-site vendor audits; SendTax relies on independent attestations and the DPA's audit-rights framework. This is standard practice for a company of SendTax's size and a deliberate scope decision.
- SendTax does not currently run automated vendor-risk-scoring tools. A formal vendor risk register and structured annual scoring is on SendTax's roadmap.

11. Vendor incidents

When an incident originates with or is exacerbated by a sub-processor, SendTax follows the process defined in the **Incident Response Policy** §13, including:

- Engaging the provider's published incident-response channel immediately
- Tracking the provider's communications on SendTax's own incident timeline
- Notifying affected customers per the Incident Response Policy regardless of whether the underlying issue was within SendTax-operated infrastructure or the sub-processor's

A vendor incident that reveals an unrecoverable gap in the vendor's security posture is grounds for emergency offboarding under §12.

12. Vendor termination and offboarding

When a vendor relationship ends — whether at SendTax's initiative, the vendor's, or by contract expiration — the offboarding process includes:

1. **Migration.** Customer data, where applicable, is migrated to a replacement vendor or back to SendTax-operated infrastructure
2. **Deletion request.** SendTax issues a formal deletion request to the vendor under the terms of the DPA. The vendor's confirmation of deletion is captured for SendTax's records
3. **Credential rotation.** All API keys, OAuth grants, and service-account credentials issued to the vendor are revoked at the source; references in SendTax secret storage are removed
4. **Sub-Processor List update.** The vendor is removed from the public list

5. **Customer notification.** Where the offboarding constitutes a material change, customers are notified per §9
6. **Documentation.** Offboarding decision, rationale, and confirmations are documented in the internal vendor inventory

Emergency offboarding (in response to a critical incident or unrecoverable security failure) follows the same steps, compressed in time, with the **Incident Commander** authorized to act with single-operator approval per the **Incident Response Policy** §5.

13. Internal vendor inventory

SendTax maintains an internal vendor inventory recording, for each vendor:

- Tier classification
- Service description and personal data categories handled
- Processing region(s)
- DPA / contract status and renewal date
- Most recent SOC 2 (or equivalent) review date
- Listing status on the public Sub-Processor List (Tier 1 only)
- Owner inside SendTax for ongoing relationship management

The inventory is reviewed at the semi-annual policy review and updated whenever a vendor changes tier, scope, region, or contractual status.

14. Exceptions

Any deviation from this policy — including, but not limited to, onboarding a vendor under §5.4, continuing a relationship with a vendor whose attestation has lapsed, or temporarily operating without a signed DPA — requires:

1. Approval from a second SendTax operator (both co-founders for §5.4 exceptions)
2. A documented justification recorded with the change
3. A defined re-evaluation point (no exception is open-ended)

Exceptions are reviewed at each policy review and are not allowed to become permanent without explicit re-authorization.

15. Enforcement

Violations of this policy may result in revocation of vendor access, termination of vendor relationship, internal disciplinary action against SendTax personnel who authorized non-compliant vendor access, and, where applicable, civil or criminal referral.

16. Related policies

- **Information Security Policy** — umbrella policy; sub-processor compliance references in §5.3
- **Access Control Policy** — third-party access controls (§7)
- **Encryption Policy** — vendor cryptographic requirements
- **Incident Response Policy** — sub-processor incident coordination (§13)
- **Data Retention & Deletion Policy** — vendor data return/destruction on offboarding
- **Privacy Policy** — customer-facing description of vendors and §7216 treatment

17. Document control

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

18. Contact

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