TRUST CENTER

Information Security Policy

The technical and operational controls SendTax uses to protect tax and identity information.

Effective: May 26, 2026 Owner: Howell & Gibbs LLC Status: v1 – initial publication

---

1. Purpose

This policy describes how SendTax protects the information it handles on behalf of tax filers and tax professionals. It is the top-level document of our security program; specific controls are detailed in the policies linked in Section 9.

SendTax processes tax documents — IRS forms, financial statements, identity documents, and related taxpayer information. We treat this data with the standard of care expected by the FTC Safeguards Rule and IRS Publication 4557, and we have built our systems on that assumption from day one.

2. Scope

This policy applies to:

- All SendTax employees, contractors, and co-founders
- All systems, services, and infrastructure operated by SendTax
- All customer data, including documents uploaded by filers and accessed by tax professionals
- All third-party services (sub-processors) that handle SendTax data on our behalf

3. Roles and responsibilities

SendTax is a small company. Security responsibility is held by the co-founders, with one named owner accountable for the program overall.

- **Security Lead (Liam Howell, Co-founder):** Owns this policy and the broader security program. Approves exceptions. Coordinates incident response. Reviews access at least quarterly.
- **Co-founder (Holly Gibbs):** Shares responsibility for vendor due diligence, customer-facing security communications, and program decisions.
- **All personnel:** Responsible for following every policy linked in Section 9, completing required security training, reporting suspected incidents promptly, and protecting credentials.

As SendTax grows, we will formalize a security committee and may appoint a dedicated security officer.

4. Information classification

SendTax handles four broad categories of information. Each is protected proportionally to its sensitivity.

Class	Examples	Default handling
Restricted	Tax documents, SSNs, financial account info, identity documents	Encrypted at rest and in transit; RLS-enforced isolation; access logged
Confidential	User account data, firm/preparer records, internal product data	Encrypted at rest and in transit; access restricted to authorized roles
Internal	Operational documents, internal communications, source code	Access restricted to personnel; not for public distribution
Public	Marketing material, this policy, our Trust Center	No restrictions

5. Security commitments

5.1 Access control

Access to SendTax systems follows the principle of least privilege. User authentication is brokered through our identity provider (Clerk, SOC 2 Type II), which supports multi-factor authentication. MFA is currently available to all users and may be enabled from account settings; required MFA for tax-professional and administrator roles is in development. Customer data is isolated at the database layer using PostgreSQL Row-Level Security (RLS) — not application-layer filtering — so that even a misbehaving query cannot return another tenant's data. Cross-tenant access (e.g., a tax professional accessing a filer's documents) is brokered through explicit, status-tracked link records, never through implicit ownership.

See: Access Control Policy.

5.2 Encryption

All customer documents are encrypted at rest using AES-256-GCM with per-document keys, wrapped via envelope encryption with a key encryption key (KEK) managed in Google Cloud KMS. Authenticated Additional Data (AAD) binds each ciphertext to its document and filer identifiers, preventing ciphertext substitution. Data in transit is protected by TLS 1.2 minimum, with TLS 1.3 preferred and negotiated where supported by the client (verified 2026-05-26 at the Fly edge via `openssl s_client` probe across send.tax, app.send.tax, pro.send.tax, admin.send.tax). HTTP Strict Transport Security is configured in every Next.js app with `max-age=63072000; includeSubDomains; preload` (see `apps/*/next.config.js`) and is observed on the `send.tax` apex and on direct content responses; submission of the apex to hstspreload.org is the remaining Phase-2 task so subdomain redirects inherit the policy from a cold browser.

See: Encryption Policy.

5.3 Infrastructure security

SendTax runs on managed infrastructure providers, each of which maintains current third-party security attestations:

- **Fly.io** (compute, managed Postgres, Redis) — SOC 2 Type II

- **Cloudflare R2** (object storage) — SOC 2 Type II, ISO 27001, ISO 27701, PCI DSS Level 1
- **Google Cloud KMS** (key management) — SOC 1/2/3, ISO 27001/27017/27018/27701
- **Clerk** (identity and authentication) — SOC 2 Type II, CCPA-compliant
- **Modal** (ML inference) — SOC 2 Type II
- **Sentry** (error monitoring) — SOC 2 Type II, ISO 27001

We do not operate our own physical data centers and rely on these providers' physical, network, and platform security controls. The full list of sub-processors, including those handling transactional email and other supporting functions, is maintained on our sub-processors page.

5.4 Secure development

Source code is managed in version control with access restricted to authorized contributors. Changes are reviewed before reaching production. Production secrets are stored in Fly.io's encrypted secret store for runtime injection and in environment-segmented 1Password vaults (`Clerk-Dev`, `Clerk-Staging`, `Clerk-Production`, `Cloudflare`, `E2E_Clerk_User`, `SystemWorker-Staging`, `SystemWorker-Production`) for operator access; provisioning scripts in `st-backend/infra/lib/common.sh` select the correct vault per environment. Secrets are never committed to source. Automated dependency scanning runs via **Dependabot** (configured in `.github/dependabot.yml` for pip, npm, GitHub Actions, and Docker base images; monthly grouped updates with security advisories opened immediately) and secret-scanning runs via **Gitleaks v8.18.4** as a pre-commit hook (see `.pre-commit-config.yaml`) plus GitHub's native secret-scanning with push protection as the server-side mirror. Static analysis (type checking, linting) is enforced as a required CI check.

5.5 Vendor and sub-processor management

Every third-party service that processes SendTax data is reviewed for security posture before adoption and tracked in our public sub-processor list. We prefer vendors with current SOC 2 or equivalent attestations.

See: Vendor Management Policy and our Sub-processor List.

5.6 Personnel security

All personnel agree to confidentiality obligations and acceptable use terms before being granted access to customer data. New personnel complete onboarding that covers data handling, credential hygiene, and acceptable use expectations. Devices used to access customer data are Apple hardware running macOS with FileVault full-disk encryption enabled and screen-lock enforced. SendTax operators currently use Apple-issued hardware (Mac Mini, MacBook Pro, MacBook Air); MDM management is not yet in place and remains on the roadmap. Personal accounts and personal devices not configured to these standards are not used for accessing customer data. Access is provisioned based on role, reviewed at least quarterly, and revoked promptly upon role change or departure as part of a documented offboarding checklist.

See: Acceptable Use Policy.

5.7 Incident response

SendTax maintains a defined process for detecting, responding to, and notifying affected parties of security incidents. We commit to notifying impacted customers without undue delay, in accordance with applicable law and our customer agreements.

See: Incident Response Policy.

5.8 Business continuity

Customer documents and metadata are backed up via our managed database provider's automated backup and point-in-time recovery. Formal recovery time and recovery point objectives are under development and will be published when finalized.

See: Business Continuity Policy.

5.9 Data retention and disposal

SendTax retains customer data only as long as needed to provide the service or as required by law, and disposes of it securely when no longer needed.

See: Data Retention & Deletion Policy.

6. Compliance and legal alignment

SendTax designs its security program with reference to:

- **FTC Safeguards Rule** (16 CFR Part 314) — applicable to us as a handler of financial information
- **IRS Publication 4557** — the safeguarding standard for taxpayer data, which our tax professional customers are also required to follow
- **SOC 2 Trust Services Criteria** — our program is aligned with the SOC 2 framework. We are not currently SOC 2 audited; we will pursue formal attestation when warranted by customer demand and company stage.
- **State data protection laws** applicable to our customers and users

7. Exceptions

Any deviation from this policy requires written approval from the Security Lead and is recorded with a defined expiration date. Exceptions are reviewed at least annually.

8. Enforcement

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

9. Related policies

- Access Control Policy
- Encryption Policy
- Incident Response Policy
- Data Retention & Deletion Policy
- Vendor Management Policy
- Acceptable Use Policy
- Business Continuity Policy
- SendTax Written Information Security Program (WISP)

10. Document control

Version	Date	Author	Notes
1.0	May 21, 2026	Holly Gibbs	Initial publication
1.1	May 26, 2026	Liam Howell	Verification text in section 5

11. Contact

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