SendTax

TRUST CENTER

Written Information Security Program (WISP)

The administrative, technical, and physical safeguards SendTax maintains under IRS Pub. 4557 / FTC Safeguards Rule.

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

Review cadence: Annual; additionally upon any material change to business operations, technical environment, or threat conditions

---

1. Purpose and authority

This Written Information Security Program ("WISP") describes the administrative, technical, and organizational safeguards SendTax maintains as a covered financial institution under the Gramm-Leach-Bliley Act (GLBA). It is the program referenced in SendTax's published **Privacy Policy**.

This document is designed to satisfy the requirements of:

- The **FTC Standards for Safeguarding Customer Information** ("Safeguards Rule"), 16 CFR Part 314 (as amended)
- **IRS Publication 4557** ("Safeguarding Taxpayer Data") and the related **Publication 5708** WISP guidance
- **IRS Publication 1345** ("Handbook for Authorized IRS *e-file* Providers"), to the extent it applies to tax-document workflows
- The **New York SHIELD Act** "reasonable safeguards" standard (N.Y. Gen. Bus. Law §899-bb)

This document does not create new security controls. It consolidates and references the security program already established in SendTax's published policies. Where this

WISP and a referenced policy disagree, the referenced policy controls; this WISP is updated to match.

Items marked **(roadmap)** are commitments SendTax is implementing; current state and timeline are documented in §14.

2. Scope

This WISP covers:

- **Customer information** as defined by the Safeguards Rule §314.2(d): any record containing nonpublic personal information about a consumer of SendTax services, in any form. This includes taxpayer identity information, financial account information, tax-return data, and supporting documents.
- **Customer information systems**: every SendTax-operated system that processes, stores, or transmits customer information, including application code, databases, document storage, and the operator endpoints used to administer them
- **Personnel**: SendTax co-founders, employees, and contractors of Howell & Gibbs LLC with any access to customer information or customer information systems
- **Service providers**: every Tier 1 sub-processor listed on the published Sub-Processor List

SendTax operates exclusively in the United States. The operating entity is Howell & Gibbs LLC.

3. Qualified Individual (§314.4(a))

Liam Howell, Co-founder, SendTax, is designated as the Qualified Individual responsible for overseeing, implementing, and enforcing this information security program.

The Qualified Individual:

- Has overall responsibility for the design, implementation, and ongoing operation of this WISP
- Has authority to make decisions about safeguards, including decisions to suspend services or accept risk during incidents

- Provides a written report to the members of Howell & Gibbs LLC at least annually, summarizing the status of this program, material risks, the results of testing, and any recommended changes (§11)
- Delegates day-to-day execution as appropriate but remains accountable
- Authorizes exceptions to policy per the documented exception processes in each underlying policy

For absences exceeding two business days, the Qualified Individual designates a delegate in writing.

The Qualified Individual is accountable to the members of Howell & Gibbs LLC (Holly Gibbs and Liam Howell), who function as the governing body for SendTax for purposes of §314.4(i).

4. Risk assessment (§314.4(b))

The Safeguards Rule requires a written risk assessment that identifies reasonably foreseeable internal and external risks to the confidentiality, integrity, and security of customer information, assesses the sufficiency of the safeguards in place, and is reassessed periodically and whenever circumstances materially change.

4.1 Method

For each identified risk, the assessment records:

- The nature of the risk (threat)
- The systems or data affected (assets)
- The likelihood and impact, qualitatively rated (low / moderate / high / critical)
- The current safeguards that address the risk
- Any residual risk and the planned remediation

4.2 Cadence

The risk assessment is reviewed and updated:

- At least annually
- Whenever a material change occurs in operations, systems, or the threat landscape
- Following any Critical-severity incident

4.3 Current status

A formal, structured, written risk assessment in the form described above is **on the roadmap, targeted within 3 months of this WISP's effective date** (§14). Until the formal document is produced, SendTax operates under the implicit risk-assessment reasoning embedded in the underlying policies, each of which describes the risks it addresses.

This is a known gap that the Qualified Individual is responsible for closing on the stated timeline.

4.4 Categories of risk addressed

Even without the formal written document, the underlying policies address risk in the following categories:

Risk category	Where addressed
Unauthorized access to customer data	**Access Control Policy**; **Encryption Policy**
Data loss or corruption	**Business Continuity & Disaster Recovery Policy**; **Data Retention & Deletion Policy**
Cryptographic compromise	**Encryption Policy**
Sub-processor compromise	**Vendor Management Policy**
Personnel error or misconduct	**Acceptable Use Policy**; **Access Control Policy**
Loss of operator availability	**Business Continuity & Disaster Recovery Policy** §7
Security incidents and breach response	**Incident Response Policy**
Privacy and data subject rights	**Privacy Policy**; **Data Retention & Deletion Policy**
User misuse of the service	**User Acceptable Use Policy**

5. Safeguards (§314.4(c))

The Safeguards Rule requires implementation of specific safeguards based on the risk assessment. Each is addressed below with the verbatim CFR requirement followed by SendTax's current controls.

5.1 Access controls (§314.4(c)(1))

Requirement: Implement and periodically review access controls, including technical and, as appropriate, physical controls, to authenticate and permit access only to authorized users.

SendTax controls: Implemented and documented in the **Access Control Policy**. Highlights:

- Default-deny baseline; principle of least privilege
- PostgreSQL Row-Level Security with `FORCE ROW LEVEL SECURITY` as the database-layer enforcement
- Three-layer authorization (Clerk authentication → application authorization → database RLS)
- Multi-factor authentication enforced on every system that supports it for SendTax personnel
- Quarterly access reviews
- Audit logging for all customer-data-access events (7-year retention)

5.2 Inventory of data, systems, and personnel (§314.4(c)(2))

Requirement: Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy.

SendTax controls:

- **Data inventory.** Categories and retention windows are documented in the **Data Retention & Deletion Policy** §3
- **Systems inventory.** Production systems documented in the **Information Security Policy** §5.3 and on the published Sub-Processor List

- **Sub-processor inventory.** Maintained on the public Sub-Processor List and in the internal vendor inventory per **Vendor Management Policy** §13
- **Personnel inventory.** Maintained internally; currently Holly Gibbs and Liam Howell only. Documented in §18 (Appendix A).
- **Device inventory.** Each operator's primary device is recorded in the personnel inventory along with full-disk encryption status. A structured device-inventory record for each named operator is **on the roadmap** (§14).

5.3 Encryption (§314.4(c)(3))

Requirement: Protect by encryption all customer information held or transmitted by the financial institution both in transit over external networks and at rest.

SendTax controls: Implemented and documented in the **Encryption Policy**:

- **In transit:** TLS 1.2 or higher on all customer-facing and service-to-service traffic
- **At rest:** AES-256-GCM envelope encryption with per-document Data Encryption Keys (DEKs), wrapped by a Key Encryption Key (KEK) held in Google Cloud KMS. AAD binding to document and filer identifiers ensures ciphertext is tied to its intended scope.
- **Key management:** Workload Identity Federation; no long-lived service-account keys reside on application servers
- **Disposal:** Per-document deletion removes the wrapped DEK along with the database row, rendering the underlying ciphertext unrecoverable from SendTax systems

A codebase audit on **May 21, 2026** confirmed no usage of any prohibited algorithm (MD5, SHA-1, DES, 3DES, RC4, TLS 1.0/1.1, SSL) in production code.

5.4 Secure development (§314.4(c)(4))

Requirement: Adopt secure development practices for in-house developed applications utilized by the financial institution for transmitting, accessing, or storing customer information, and procedures for evaluating, assessing, or testing the security of externally developed applications utilized to transmit, access, or store customer information.

SendTax controls: Implemented and documented in the **Information Security Policy** §5.4 and the **Change Management Policy**:

- Pre-commit hooks enforce format, type, and quality checks
- Continuous integration runs lint, type-check, and full test suites on every pull request; CI passage is required for merge
- Sensitive-area changes (encryption, RLS, authentication, audit log) require explicit area-owner acknowledgment
- Production deploys flow through a single, audited release workflow that gates production behind a staging run of the same artifact
- External dependencies are scanned automatically for known vulnerabilities

5.5 Multi-factor authentication (§314.4(c)(5))

Requirement: Implement multi-factor authentication for any individual accessing any information system, unless the Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls.

SendTax controls:

- **For SendTax personnel (operator MFA):** Implemented. MFA is required for every supporting Tier 1 vendor system (GitHub, Fly.io, Cloudflare, Google Cloud, Clerk admin, Sentry, Postmark, Stripe, 1Password, Modal, PostHog). This is current state.
- **For customers (filer and tax-professional MFA):** MFA is **available** via Clerk; users may enable it from account settings. **Enforced MFA for the Preparer, Viewer, and Firm Administrator roles shipped 2026-05-28**, four months ahead of the September 2026 target. The resolver at `st-backend/app/core/mfa.py` reads Clerk's `fva` session-token claim to detect enrollment, soft-blocks non-compliant logins inside a per-user 14-day grace window (logged + emailed), and hard-blocks with HTTP 403 (`error_code = mfa_enrollment_required`) once grace expires. Every soft-block, hard-block, enrollment observation, grace extension, and tenant-policy change writes a discrete audit-log row. Filer accounts remain opt-in. This closes the previous §5.5 roadmap item.

5.6 Disposal of customer information (§314.4(c)(6))

Requirement: Develop, implement, and maintain procedures for the secure disposal of customer information no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or other

legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

SendTax controls: Documented in the **Data Retention & Deletion Policy**. Highlights:

- Defined retention periods for each data category, including 7 years for service data (consistent with AICPA professional guidance and IRS audit-window considerations, justified as necessary for legitimate business operations) and IRS-aligned retention for e-file authorization records
- Per-document cryptographic disposal via wrapped-DEK removal
- Customer rights to access, correction, and deletion, subject to applicable legal-retention obligations
- Automated hard-deletion of soft-deleted accounts is **on the roadmap** (Retention Policy §9); interim hard deletions are processed manually

5.7 Change management (§314.4(c)(7))

Requirement: Adopt procedures for change management.

SendTax controls: Implemented and documented in the **Change Management Policy**. Production changes require:

- Pull request review and approval
- CI passing on the merge commit
- Deploy through the audited release workflow (`release.yml`); no manual production access for routine changes

5.8 Activity monitoring (§314.4(c)(8))

Requirement: Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

SendTax controls: Documented in the **Access Control Policy** §8:

- Application-level audit logs for sensitive actions (retained for a minimum of 7 years)
- Authentication event logs (via Clerk)
- Infrastructure event logs (via Fly.io, Google Cloud, Cloudflare)

- Error and performance telemetry (via Sentry)

SendTax does not currently operate a centralized SIEM with continuous real-time monitoring. A more proactive monitoring posture is on the roadmap (§14).

6. Testing and monitoring (§314.4(d))

The Safeguards Rule requires regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures. Where continuous monitoring is not used, annual penetration testing and biannual vulnerability assessments are required.

6.1 Current state

SendTax does not currently operate continuous monitoring meeting §314.4(d)(1). Accordingly, SendTax is electing the §314.4(d)(2) path: annual penetration testing and biannual vulnerability assessment.

Neither penetration testing nor formal vulnerability assessment has yet been conducted. Both are on the roadmap (§14):

- First vulnerability assessment: within 6 months
- First penetration test: within 12 months
- Vulnerability assessment biannual cadence: established after first assessment

6.2 What is currently in place

While the formal §314.4(d)(2) program is being established, the following activities provide ongoing visibility (these do not substitute for §314.4(d)(2) but supplement it):

- **Application health checks** continuously polled by Fly.io and alerting on failure
- **Dependency scanning** in CI on every pull request
- **Secret-scanning** in CI on every pull request
- **Error and performance telemetry** flowing to Sentry, reviewed in response to alerts or incidents
- **Authentication telemetry** via Clerk (sign-in events, failed attempts, suspicious patterns)
- **Access reviews** quarterly per the **Access Control Policy** §5.5
- **Tabletop exercises** on roadmap per the **Incident Response Policy** §15

6.3 Privacy Policy reconciliation

SendTax's published Privacy Policy currently references alignment with IRS Pub 1345 expectations, including "weekly external ASV scans" and an "EV TLS certificate." Per §12.2, these controls are **not currently in place** and are on the roadmap. This WISP is the authoritative source on current control status; the Privacy Policy will be reconciled to match.

7. Personnel security and training (§314.4(e))

The Safeguards Rule requires utilization of qualified information-security personnel, providing them with security-awareness training, and verifying that key personnel maintain current knowledge of changing security threats.

7.1 Training requirements (defined in the Acceptable Use Policy §2)

- All SendTax personnel must read and acknowledge the **Acceptable Use Policy** before being granted access to customer data
- Re-acknowledgment is required at each material policy update
- A documented annual training topic, selected by the Qualified Individual based on current threat conditions, is delivered to all personnel
- The Qualified Individual maintains current knowledge through industry publications, FTC and IRS guidance updates, and security-vendor advisories

7.2 Current personnel

SendTax personnel currently consists of Holly Gibbs and Liam Howell. Both will acknowledge the **Acceptable Use Policy** before publication of this WISP. When SendTax engages additional personnel (employees, contractors, advisors with system access), this WISP applies and acknowledgment is required as part of onboarding.

7.3 Annual training records

Documented annual security-awareness training with completion records for all personnel is **on the roadmap** (§14) and will be in place before the first annual report to the governing body (§11).

8. Sub-processor oversight (§314.4(f))

The Safeguards Rule requires overseeing service providers by (1) taking reasonable steps to select and retain providers capable of maintaining appropriate safeguards; (2) requiring providers by contract to implement and maintain such safeguards; and (3) periodically assessing such providers based on the risk they present and the continued adequacy of their safeguards.

SendTax controls: Documented in the **Vendor Management Policy**:

- Three-tier vendor model (Tier 1 sub-processors, Tier 2 operational vendors with incidental access, Tier 3 internal-only tools)
- Pre-onboarding due diligence appropriate to tier, including review of SOC 2 Type II or equivalent attestations
- Defined §5.4 exception path for Tier 1 vendors lacking direct attestation but covered by parent-company attestation
- Contractual requirements including Data Processing Agreements, breach notification, sub-processor disclosure, and (where applicable) IRC §7216 auxiliary-service notice
- Annual review of Tier 1 sub-processors; biennial review of Tier 2; event-driven review of Tier 3
- Public Sub-Processor List with 30-day advance notice of material changes

SendTax operates U.S.-only; all current Tier 1 sub-processors are U.S.-based.

9. Incident response (§314.4(h))

The Safeguards Rule requires a written incident response plan addressing specific elements. SendTax's plan, documented in the **Incident Response Policy**, addresses each:

§314.4(h) element	Where addressed
Goals of the plan	IR Policy §1, §2
Internal processes for responding	IR Policy §6, §7
Roles, responsibilities, decision authority	IR Policy §5

External and internal communications	IR Policy §7.5, §9
Identification of weaknesses in systems and controls	IR Policy §11, §12
Documentation and reporting of security events	IR Policy §11
Post-incident evaluation	IR Policy §12

9.1 Notification obligations

The **Incident Response Policy** §10 commits SendTax to the following notification timelines:

- **FTC Safeguards Rule notification (§314.4(j)):** Within 30 days of discovery of a notification event affecting 500 or more consumers
- **IRS reporting:** Next-business-day reporting to the IRS Stakeholder Liaison for incidents affecting taxpayer data, consistent with IRS Publication 1345
- **State-law notification:** Per applicable state breach-notification statutes, including NY SHIELD Act
- **Customer notification:** Within 72 hours of confirmed incidents affecting customer data
- **Affected sub-processor notification:** Per **Vendor Management Policy** §11

10. Evaluate and adjust (§314.4(g))

The Safeguards Rule requires evaluating and adjusting the information security program in light of testing results, material changes, risk assessment results, or other material circumstances.

SendTax controls: Every policy in this batch carries an explicit review cadence (semi-annual default) and a list of triggers for out-of-cycle review. The Qualified Individual is responsible for ensuring the program is updated when any trigger fires.

A combined annual review of every Trust Center document and the underlying internal evidence is conducted before each annual report to the governing body.

11. Annual report to governing body (§314.4(i))

The Safeguards Rule requires the Qualified Individual to report in writing, regularly and at least annually, to the board of directors or equivalent governing body on the overall status of the program; material risk-related matters; risk-management decisions; service-provider arrangements; results of testing; security events and management's response; and recommendations for changes.

For Howell & Gibbs LLC, the members (Holly Gibbs and Liam Howell) function as the governing body. The Qualified Individual produces a written **Annual WISP Report** addressed to the members.

The first report will be issued no later than May 21, 2027 (within twelve months of this WISP's effective date) and annually thereafter.

Each report covers, at minimum:

- Status of each safeguard in §5
- Results of testing and monitoring during the period (§6), including any pen-test or vulnerability-assessment results once those programs are in place
- Status of each item on the WISP roadmap (§14), including items that have shipped during the period and any new items added
- Material changes to operations, systems, or sub-processors
- A summary of any Critical or High-severity incidents during the period, with links to incident records and any postmortems
- Recommendations for changes to this WISP

Completed annual reports and the governing body's acknowledgments are retained per the **Data Retention & Deletion Policy** §3.6 (audit logs and security records).

12. Tax-data-specific overlay (IRS guidance)

12.1 IRS Publications 4557 and 5708

This WISP is structured to satisfy the WISP-template guidance in IRS Publication 4557 ("Safeguarding Taxpayer Data") and Publication 5708 ("Creating a Written Information Security Plan for Your Tax & Accounting Practice"). The mapping of Pub 5708 sections to this WISP is maintained internally for audit and is available on request.

12.2 IRS Publication 1345 (e-file ecosystem)

For tax-document workflows that interact with the IRS e-file ecosystem, SendTax aligns with the security expectations of IRS Pub 1345. The current status of each expectation is:

Pub 1345 expectation	Status
Public-facing tax sites secured with an Extended Validation (EV) TLS certificate	**Roadmap.** Current certificates are managed by Fly.io's edge (typically standard DV). The Privacy Policy references EV alignment; this WISP is the authoritative source that EV certificate procurement is in development.
External vulnerability scans on a weekly cadence (Approved Scanning Vendor scans)	**Roadmap.** See §6.1 and §14. Privacy Policy implies these are in place; this WISP is the authoritative source that they are not yet in place.
U.S. domain registration	In place. `send.tax` is registered through a U.S. registrar.
Next-business-day incident reporting to the IRS for events affecting e-file or tax-data systems	Committed; operational responsibility sits with the Communications Lead during incident response (IR Policy §10)
Retention of IRS-required e-file records (e.g., Forms 8878 and 8879) for three years	In place. See **Data Retention & Deletion Policy** §3.2.

12.3 PTIN and Circular 230

Tax professionals using SendTax are required to hold a valid PTIN and comply with Treasury Circular 230. The PTIN obligation is enforced at the data-model level: the `preparers.ptin` column is non-nullable and has a unique constraint. Circular 230 compliance is the responsibility of the individual preparer; SendTax facilitates but does not validate it. The user-facing commitments are documented in the **User Acceptable Use Policy** §6.

13. New York SHIELD Act alignment

The New York SHIELD Act (N.Y. Gen. Bus. Law §899-bb) requires "reasonable safeguards" — administrative, technical, and physical. The safeguards described in §5 of this WISP, together with the operational practices in §6–§9, are designed to satisfy the SHIELD Act's "reasonable safeguards" standard for any New York resident whose private information is processed by SendTax.

14. Roadmap commitments

The following commitments are required for full §314.4 compliance and are being implemented. Each is listed with the gap and the indicative timeline. Once each commitment is implemented, this WISP will be revised to reflect current state and the corresponding line removed.

Commitment	§314.4 element	Target
Formal written risk assessment	§314.4(b)	Within 3 months of WISP effective date
First vulnerability assessment	§314.4(d)(2)	Within 6 months of WISP effective date
First penetration test	§314.4(d)(2)	Within 12 months of WISP effective date
Vulnerability assessment biannual cadence	§314.4(d)(2)	Established after first assessment
Documented annual security-awareness training with completion records	§314.4(e)	Within 12 months of WISP effective date
First annual report to governing body	§314.4(i)	Within 12 months of WISP effective date (by May 21, 2027)

~~Customer MFA enforcement for tax-professional users and administrators~~ **SHIPPED 2026-05-28**	§314.4(c)(5)	~~Target: 2026-09-26~~ Shipped 2026-05-28 (4 months ahead). Backend enforcement at `st-backend/app/api/routes/auth.py` via the resolver in `st-backend/app/core/mfa.py`, gated on `tenant.require_mfa` plus per-role check. 14-day per-user grace window; audit-logged soft/hard blocks. Frontend banner + Security page wired in `st-apps/apps/pro-web`. See §5.5 above for the steady-state description.
Structured device-inventory record for each named operator	§314.4(c)(2)	Within 6 months of WISP effective date
EV TLS certificate procurement (Pub 1345 alignment)	Pub 1345 §12.2	Within 6 months of WISP effective date
Weekly Approved Scanning Vendor (ASV) scans (Pub 1345 alignment)	Pub 1345 §12.2	Within 6 months of WISP effective date
Privacy Policy reconciliation (retention period, advance-notice claim, sub-processor list completeness, EV/ASV claims, entity name, contact domain)	Cross-policy	Before WISP publication
Continuous monitoring posture (optional alternative to §6.1 path)	§314.4(d)(1)	Longer-term

In addition, this WISP inherits the roadmap commitments documented in the underlying policies (notably the Data Retention roadmap items in §9 of that policy, the

Business Continuity roadmap items in §11 of that policy, and the Vendor Management vendor inventory work in §13 of that policy).

15. Compliance framework alignment

This WISP and its underlying policies are designed to satisfy multiple overlapping compliance frameworks:

Framework	Where addressed
FTC Safeguards Rule (16 CFR Part 314)	This WISP; underlying policies
Gramm-Leach-Bliley Act (GLBA)	This WISP; **Privacy Policy**; **Data Retention & Deletion Policy** §5.2
IRC §7216 (federal restrictions on tax return information)	**Privacy Policy**; **User Acceptable Use Policy** §6; **Vendor Management Policy** §7.2; **Acceptable Use Policy** §10
IRS Publication 4557	This WISP §12.1; **Information Security Policy**
IRS Publication 5708	This WISP §12.1
IRS Publication 1345	This WISP §12.2; **Privacy Policy**; **Incident Response Policy** §10; **Data Retention & Deletion Policy** §3.2
NY SHIELD Act	This WISP §13; **Privacy Policy**; **Incident Response Policy** §10
State consumer privacy laws (CCPA/CPRA, VCDPA, CPA, CTDPA, UCPA, and others)	**Privacy Policy**; **Data Retention & Deletion Policy** §5
SOC 2 Common Criteria and Trust Services Criteria	All policies cross-reference relevant CC and TSC criteria

16. Companion documents

This WISP is the umbrella program; the controls it describes are implemented and operationalized through the following companion policies and standards, each published on the SendTax Trust Center:

1. **Information Security Policy** — umbrella policy
2. **Access Control Policy** — identity, authorization, audit logging
3. **Encryption Policy** — cryptographic standards and key management
4. **Incident Response Policy** — incident handling and notification
5. **Data Retention & Deletion Policy** — retention periods and disposal mechanisms
6. **Vendor Management Policy** — sub-processor oversight
7. **Acceptable Use Policy** — personnel-facing rules
8. **Business Continuity & Disaster Recovery Policy** — availability and recovery
9. **User Acceptable Use Policy** — user-facing rules
10. **Change Management Policy** — production-change governance

Plus the customer-facing **Privacy Policy** and **Sub-Processor List**.

17. Exceptions and enforcement

Any deviation from the program described in this WISP requires approval by the Qualified Individual, documented justification, and a defined re-evaluation point. Material exceptions are reported to the governing body at the annual review (§11).

Violations of this WISP or any underlying policy are subject to enforcement per the relevant underlying policy and may result in revocation of access, termination of employment or contract, and, where applicable, civil or criminal referral.

18. Appendix A — personnel with access to customer information

Name	Role	Access scope
Liam Howell	Co-founder; Qualified Individual; production deploy access	Full administrative access to all systems
Holly Gibbs	Co-founder; admin dashboard access; break-glass production deploy access on roadmap per BCP §9.3	Full administrative access to non-production systems and admin dashboard

Updates to this appendix are made when personnel join, change role, or depart.

19. Appendix B — systems holding customer information

The current list of Tier 1 sub-processors is maintained on the public Sub-Processor List. Summary:

- Fly.io — application hosting and managed Postgres
- Cloudflare R2 — document object storage
- Google Cloud KMS — Key Encryption Key custody
- Clerk — identity and authentication
- Resend — transactional and inbound email
- Modal — ML inference
- Sentry — error monitoring
- PostHog — product analytics (configured without individual user tracking)
- Stripe — payment processing

Tier 2 (operational vendors with incidental access) and Tier 3 (internal-only tools) are tracked in the internal vendor inventory per **Vendor Management Policy** §13.

20. Document control

Version	Date	Author	Notes
1.0	May 21, 2026	Holly Gibbs	Initial publication
1.1	May 28, 2026	Liam Howell	§5.5 and §14: customer MFA enforcement shipped for Preparer, Viewer, and Firm Administrator roles — four months ahead of the original target. Cascade edit lands in ACP §4.1 / §5.1 (ACP v1.2).

21. Contact

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