TRUST CENTER

# Access Control Policy

Review cadence: Semi-annual, or after any material change to access patterns or systems

Effective: June 4, 2026 Owner: Howell & Gibbs LLC Status: V1.3 – initial publication

---

## 1. Purpose

This policy defines how SendTax grants, manages, and revokes access to its systems and customer data. It covers both internal access (SendTax personnel accessing production systems and customer data) and customer-facing access (how filers and tax professionals are authenticated and how their data is isolated from one another).

This policy supports the commitments made in the Information Security Policy and aligns with SOC 2 Common Criteria CC6.1–CC6.8.

## 2. Scope

This policy applies to:

- All SendTax personnel (employees, contractors, co-founders) accessing any SendTax system
- All third parties granted access to SendTax production systems or customer data
- All customer-facing access by filers and tax professionals to the SendTax application
- All systems storing or processing customer data, including production infrastructure, source code repositories, secrets management, observability tools, and the SendTax admin dashboard

## 3. Principles

SendTax operates its access control program on five principles:

- **Least privilege.** Every identity — human or service — receives the minimum access required for its purpose, and nothing more.
- **Need-to-know.** Access to customer data is granted only where there is a specific operational, support, or legal need, and is time-bound where possible.
- **Default deny.** New roles, new tables, and new endpoints start with no access. Permissions are added deliberately, not removed reactively.
- **Separation of identities.** Production and non-production access use distinct credentials. Personal and company accounts are kept separate.
- **Defense in depth.** Access is controlled at multiple layers — identity provider, application, and database — so that a failure at any one layer does not result in unauthorized access. Client-side controls are treated as user-experience affordances, never as security boundaries.

## 4. Customer-facing access control

### 4.1 Authentication

Customer authentication is brokered through **Clerk**, our identity provider (SOC 2 Type II). Clerk handles:

- Password storage (bcrypt hashing), breach-password detection, and rate-limiting
- Session management via short-lived JWTs validated server-side against Clerk's signing keys on every authenticated request
- Multi-factor authentication options (TOTP and authenticator apps)
- Account recovery flows

**MFA is available** to every SendTax account and can be enabled at any time from account settings. **MFA is required and enforced server-side** for the Preparer, Viewer, and Firm Administrator roles, shipped 2026-05-28. Enforcement reads the Clerk session token's `fva` claim to detect enrollment; non-enrolled tax-professional logins are soft-blocked (logged, allowed to proceed) during a 14-day per-user grace window starting on first observation, then hard-blocked with HTTP 403 (`error_code = mfa_enrollment_required`). Filer accounts remain opt-in. The resolver lives at

`st-backend/app/core/mfa.py`; the kill-switch and grace duration are controlled by `MFA_ENFORCEMENT_ENABLED`, `MFA_ENFORCED_ENVIRONMENTS`, and `MFA_GRACE_PERIOD_DAYS`.

### 4.2 Authorization and tenant isolation

SendTax recognizes four customer-facing roles, enforced server-side:

| Role | Identity | What they can access |
|---|---|---|
| **Filer** | An individual taxpayer with a SendTax account | Their own profile, documents, returns, and obligations |
| **Preparer** | A staff member of a tax-professional firm with an active link to a filer | The filer's documents and return data, scoped to the active relationship; full preparation capability |
| **Viewer** | A staff member of a firm with read-only access to a linked filer | Read-only access to the filer's documents and return data |
| **Firm Administrator** | A tax-professional account with authority to manage their firm's staff and filer relationships | Firm-level configuration, staff role assignment, and filer-link lifecycle within their own firm only |

Customers cannot escalate their own role. The Preparer/Viewer distinction is recorded in the `tenant_filer_links` table and enforced at the database layer — the tenant write policies require a `PREPARER` link, so a Viewer link is read-only at the database itself, with a matching application-layer guard. The **Firm Administrator** vs. member distinction is enforced server-side by a `require_firm_admin` check on firm-management actions (staff management and the firm's filer-link lifecycle); a firm-staff invite/accept flow lets a firm have more than one user.

Authorization is enforced at three layers, in order:

1. **Identity provider (Clerk).** The request must present a valid, unexpired JWT.

2. **Application layer.** API endpoints declare which role(s) may invoke them. Internal-only endpoints are guarded by an explicit `require_admin` dependency that verifies elevated privilege server-side.
3. **Database layer.** PostgreSQL Row-Level Security (RLS) is the final authoritative check. Specifically:
    - Every customer-data table has RLS policies defined with `FORCE ROW LEVEL SECURITY`, meaning the policies are enforced even for the database owner role. An application bug cannot return another tenant's rows.
    - Each authenticated request sets one of two mutually exclusive PostgreSQL session variables before any query runs: `app.tenant_id` (a firm acting on a filer's behalf) or `app.filer_id` (a filer acting on their own data).
    - RLS policies on every table reference these session variables. The database itself returns only rows the caller is authorized to see.
    - The application connects to PostgreSQL using a non-superuser role; superuser-level connections are not used in application code paths.

A bug in any single layer does not, by itself, expose another customer's data.

### 4.3 Cross-tenant access and customer-controlled lifecycle

Tax professionals do not have ambient access to filer data. Access is brokered through an explicit `tenant_filer_links` table, which records the relationship between a firm and a filer with one of four lifecycle states:

- **Pending** — invitation extended by the firm; the filer has not yet accepted. The firm has no access to the filer's data in this state.
- **Active** — the filer has accepted; access is permitted in accordance with the staff member's role (Preparer or Viewer).
- **Ended** — terminated by either party. The firm's access — including for staff currently signed in — is revoked on the next authenticated request, because authorization is checked at the database level on every query.
- **Suspended** — temporarily disabled for compliance or billing reasons. Produces the same access revocation as Ended.

Only links in the **Active** state grant access. State transitions are recorded with timestamps. Filers control their own relationships: they can terminate any link at any time from their account, and revocation takes effect immediately.

### 4.4 Object storage access

Customer documents are stored in Cloudflare R2 and partitioned by `filer_id` in the storage path. Application-layer access is mediated by signed URLs with short expiration windows; direct public access to the storage bucket is not permitted.

### 4.5 Customer account provisioning

Customer accounts are provisioned automatically through self-serve signup, mediated by Clerk. New users authenticate themselves through standard Clerk flows (email/password, MFA-eligible), and accounts are created with the appropriate role (filer or tax professional) determined by the signup context. No SendTax personnel action is required to create a customer account.

During SendTax's Early Access Program, SendTax personnel do not create accounts directly — they create an invitation that pre-populates a standard Clerk self-serve signup, which the invitee completes themselves. This invite flow includes duplicate-account checks and tracked delivery; it does not bypass Clerk authentication or alter the underlying access model described in Sections 4.1–4.3.

### 4.6 Customer account deletion

Customers can delete their own SendTax account from inside the product at any time. The "Delete account" affordance lives in **Settings → Account** in both the filer web app and the pro web app and is surfaced as a link in the authenticated footer. Confirming the deletion requires the customer to type the word `DELETE` so a single click cannot trigger an irreversible action.

In-product deletion calls `DELETE /api/v1/auth/me`, which writes a `self_service_delete` audit row attributed to the principal *before* calling Clerk's admin API to remove the user. Clerk then fires a `user.deleted` webhook back to SendTax which (a) marks the SendTax-side `User` or `Filer` mirror record as `is_active=false`, (b) revokes all of the principal's active sessions, and (c) records a second audit row tagged `source=clerk_webhook`. The same Clerk webhook also handles deletions initiated from Clerk's hosted account UI, which remains available as a fallback path.

From the customer's perspective deactivation is immediate and irrevocable through the product. The data-retention process described in the **Data Retention & Deletion**

**Policy** then runs against the inactive record. Customers who delete their account in error can email `privacy@send.tax` within the soft-delete window to request restoration; once the retention window expires, the underlying data is gone and restoration is no longer possible.

*Shipped May 27, 2026.*

## 5. Internal access control

### 5.1 Authentication for personnel

SendTax personnel access several distinct systems. Authentication follows these rules:

- **Clerk** is SendTax's identity provider for the SendTax product itself, including any admin interfaces built into the product.
- **Infrastructure providers** (GitHub, Google Cloud, Fly.io, Cloudflare, 1Password, Sentry, Modal, Postmark, corporate email) are accessed via per-vendor authentication. SendTax does not currently operate a central SSO identity provider for these tools; we will adopt one when team size warrants the additional management overhead.

In all cases, the following requirements apply:

- A unique individual account per person — no shared credentials
- Strong, unique passwords stored in a password manager (1Password)
- **Multi-factor authentication, required for SendTax personnel on every system that supports it** — including each of the providers named above. For customers, MFA is *available* via Clerk for every account and *required* — server-side enforced — for the Preparer, Viewer, and Firm Administrator roles (shipped 2026-05-28). Closes the previous WISP §5.5 roadmap item.
- Personal accounts and personal devices that do not meet our device security baseline are not used to access customer data or production systems

### 5.2 Role-based access (RBAC)

Internal access is granted based on role. At SendTax's current size, the role model is intentionally simple:

| Role | Description | Typical access |
|---|---|---|
| **Security Lead / Technical Co-founder** (Liam) | Owns the security program, production infrastructure, and technical operations | All systems including production deploy access, infrastructure providers, database, and admin dashboard |
| **Co-founder, Operations & Customer-facing** (Holly) | Owns customer provisioning, support, vendor and security communications, and program decisions | Admin dashboard (full access), infrastructure providers (read/admin as needed for vendor management); no production deploy access |
| **Engineer (future)** | Contributors with production responsibilities | Production read/write as needed, scoped per system |
| **Support / Operations (future)** | Personnel with customer-facing duties but no infrastructure responsibilities | Admin dashboard (scoped to support functions); no direct database access |

Both co-founders — and only the co-founders — have access to the admin dashboard. The admin dashboard is itself an access-controlled internal application: actions performed in the dashboard are tied to the individual co-founder's authenticated identity and logged.

As SendTax grows, additional roles will be defined and the role-to-system mapping documented in an access control matrix.

### 5.3 Privileged access

The following are treated as privileged actions, requiring named human approval and a recorded justification:

- **Production deployments** — at SendTax's current size, production deploy access is restricted to a single co-founder (Liam Howell). Holly Gibbs does not have production deploy access. Production deploys are performed from a CI pipeline on a pull-request-based merge to `main`. Independent pre-merge review is not enforced at current team size — branch protection requiring reviews needs a paid GitHub plan, and a two-person team cannot

independently review the deploying co-founder's own changes — so the compensating controls are the CI quality gates, the append-only audit trail, a self-review checklist, and the privileged-action log for ad-hoc or incident deploys.

- **Production database access** — direct queries against live customer data outside of application code paths
- **Decryption operations against the production Key Encryption Key**
- **Granting or modifying SendTax personnel access**
- **Promoting an application account to elevated privileges** — performed via a deliberate scripted operation (not a UI toggle) so the action is recorded and reviewable
- **Changes to RLS policies, encryption configuration, or the secrets management system**

Customer account provisioning is not a privileged action under this section: customer accounts are created automatically through self-serve signup (see §4.5).

At SendTax's current size, privileged-action approval is lightweight but recorded in a dedicated channel-of-record: the acting operator logs the action and its justification in the **privileged-action log** in the admin Compliance dashboard (an append-only table mirrored to the audit log), and the other co-founder acknowledges it there — a person cannot acknowledge their own entry. Entries can be recorded from the dashboard or via the `record-privileged-action` Claude skill. As the team grows, this will be formalized into a request-and-approval workflow.

Long-lived shared admin credentials are not permitted. Each operator acts under their own identity.

### 5.4 Account lifecycle (Joiner-Mover-Leaver)

**Onboarding (Joiner).** New personnel are provisioned with the minimum access required for their role. Account creation is documented. Onboarding includes acknowledgment of the **Acceptable Use Policy** and confirmation that device security requirements are met.

**Role changes (Mover).** When a person's role changes, their access is re-evaluated promptly and adjusted to match their new responsibilities. Previously granted access that is no longer needed is revoked, not retained "just in case."

**Offboarding (Leaver).** When a person departs SendTax — or a contractor's engagement ends — access is revoked promptly across all systems via a documented checklist. Personal-device data wipe (where applicable) and credential rotation for any shared resources follow the same checklist.

### 5.5 Access reviews

The Security Lead conducts an access review at least **quarterly**. Each review confirms:

- Every active account is held by a current person in a current role
- The access level for each account matches their role
- No dormant or orphaned accounts exist
- Privileged access grants remain justified

Findings are remediated promptly. Reviews are documented (date, scope, findings, actions taken) and retained.

### 5.6 Device and remote-access requirements

- Devices used to access customer data and production systems run macOS with **FileVault** full-disk encryption enabled and screen-lock enforced. SendTax personnel currently work on Apple-issued hardware (Mac Mini, MacBook Pro, MacBook Air).
- Personal accounts are not used for production access; all internal systems are accessed under company-issued identities.
- Remote work is the default; there is no privileged "office network." Access controls do not depend on network location.

## 6. Service accounts and machine identities

Non-human identities (service accounts, API tokens, deploy keys) are subject to the same principles as human identities:

- Scoped to the minimum permissions required
- Documented (purpose, owner, expiration)
- Stored in our secrets management system, never in source code
- Rotated on a defined schedule — at least **annually** — and immediately upon suspected compromise
- Logged when used for privileged actions where possible

## 7. Third-party access

Where third parties (vendors, contractors, auditors) require access to SendTax systems:

- Access is granted only after a documented business need and (where applicable) a confidentiality agreement
- Access is scoped to the minimum required and time-bound
- Access is revoked promptly when the engagement ends
- Sub-processor access to customer data through their normal service operation is governed by the **Vendor Management Policy** rather than this policy

## 8. Logging and monitoring

SendTax maintains a server-side **audit log** for sensitive actions, including:

- **Authentication events** — sign-ins, sign-outs, MFA challenges, and failed attempts (captured by Clerk)
- **Tenant/filer relationship changes** — link creation, role assignment, termination, suspension
- **Administrative actions** — promotion to elevated roles, and ad-hoc privileged actions recorded in the privileged-action log (§5.3). (SendTax has no support-impersonation feature today; this bullet will expand if one is added.)
- **Access to sensitive customer data** — document access, tax-return data access
- **Infrastructure changes** — deploys, configuration changes, database access (captured by hosting provider audit logs: Fly.io, Google Cloud, Cloudflare)

Audit-log records are append-only at the application layer and stored in a dedicated table with hardened write paths. Application-level audit logs are retained for **a minimum of 7 years**, with retention of customer-data-access events extended consistent with applicable tax-data retention obligations. Specific retention periods by log category are defined in the **Data Retention & Deletion Policy**.

Operational telemetry (errors, latency, request volume) is captured by Sentry. This telemetry is scrubbed of known sensitive fields before transmission.

We do not currently operate a centralized SIEM with continuous monitoring; logs are reviewed in response to incidents, customer reports, or as part of scheduled access reviews. A more proactive monitoring posture is on our roadmap.

## 9. Exceptions

Any deviation from this policy (for example, a temporary grant of elevated access during an incident) requires:

1. Approval from a second SendTax operator
2. A documented justification recorded with the change
3. A scheduled expiration date

Exceptions are reviewed at the next access review and are not allowed to become permanent without explicit re-authorization.

## 10. Enforcement

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

## 11. Related policies

- **Information Security Policy** — umbrella policy that this document supports
- **Acceptable Use Policy** — personnel obligations when using SendTax systems
- **Encryption Policy** — how the keys this policy controls access to are managed
- **Incident Response Policy** — what happens when access controls fail or are **bypassed**
- **Vendor Management Policy** — controls for sub-processor access to customer data

## 12. Document control

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

| | | | |
|---|---|---|---|
| 1.1 | May 27, 2026 | Liam Howell | §4.6 updated: in-product "Delete account" affordance shipped (PR #75); section rewritten from roadmap to current-state. |
| 1.2 | May 28, 2026 | Liam Howell | §4.1 and §5.1 updated: customer MFA enforcement shipped for Preparer, Viewer, and Firm Administrator roles. Closes the WISP §5.5 roadmap item. Resolver at `st-backend/app/core/mfa.py`; 14-day per-user grace window with audit-logged soft/hard blocks. |
| 1.3 | June 4, 2026 | Liam Howell | §4.2 Viewer read-only + Firm Administrator/member enforcement; §5.3 privileged-action log + reviewed-PR softening; §6 annual rotation cadence; §4.5 EAP corrected to invite-pre-populates-signup. Shipping in PRs #134, #135, #136. |

## 13. Contact

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