SendTax

TRUST CENTER

Employee Acceptable Use Policy

The rules that govern use of SendTax by filers, tax-pro firms, and operators.

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

Review cadence: Semi-annual, or after any material change to personnel obligations or systems in use

---

1. Purpose

This policy defines how SendTax personnel may use the company's systems, accounts, devices, and information. It exists to:

- Protect customer data and SendTax systems from harm caused by personnel behavior
- Satisfy compliance obligations under the FTC Safeguards Rule, IRC §7216, SOC 2 (CC6.1), and applicable state laws
- Give SendTax a documented, enforceable basis for action when rules are violated

This policy supports the commitments made in the **Information Security Policy** and complements the **Access Control Policy**, **Encryption Policy**, **Incident Response Policy**, and **Data Retention & Deletion Policy**.

2. Scope and acknowledgment

This policy applies to all SendTax personnel — co-founders, employees, contractors, consultants, and any other person granted access to SendTax systems or customer data.

All personnel must acknowledge this policy in writing before being granted access to SendTax systems, and re-acknowledge it at each policy update. Acknowledgments are recorded internally and retained per the **Data Retention & Deletion Policy**.

3. Principles

- **Customer data is not yours.** Personnel may access customer data only to perform a defined operational, support, or legal task — never out of curiosity, never for personal benefit, never for any purpose other than serving the customer or operating SendTax.
- **Default-deny applies to people too.** Personnel access only what they need for the task at hand, and stop there.
- **Tax data is regulated data.** Personnel handling taxpayer information are subject to IRC §7216 and FTC Safeguards Rule obligations. Violations carry civil and potentially criminal exposure beyond ordinary employment consequences.
- **You are responsible for output, regardless of how it was produced.** This applies to AI-assisted work, automation, and anything else: the person who shipped the work owns the result.

4. Acceptable use

Personnel may use SendTax systems, accounts, and information to:

- Perform their assigned role at SendTax
- Communicate with customers, sub-processors, and other authorized parties on SendTax's behalf
- Access, modify, or transmit customer data when operationally necessary and within the scope of their role
- Develop, test, deploy, and operate the SendTax product
- Collaborate with other personnel using approved channels (§7)
- Use approved AI tools subject to the restrictions in §8

5. Prohibited activities

Personnel must not:

- Access customer data beyond what is needed for a specific operational task
- Disclose customer data to any unauthorized party

- Share credentials, access tokens, or MFA codes with any other person — including other personnel
- Use shared logins, generic accounts, or shared credentials for any production system
- Attempt to bypass or disable security controls (RLS, MFA, audit logging, encryption)
- Store production secrets or customer data on personal devices outside of approved tooling
- Transmit customer documents, taxpayer data, credentials, or production secrets over personal communication channels
- Use SendTax systems for personal profit, business activities unrelated to SendTax, or any unlawful purpose
- Install unauthorized software on company-managed systems where company-managed systems are in use
- Use AI tools in violation of the restrictions in §8
- Misrepresent themselves as another person, including other SendTax personnel, customers, or sub-processor representatives

6. Device and endpoint security

- Customer data and production systems may be accessed only from devices that meet SendTax's device security baseline:
  - Full-disk encryption enabled (Apple FileVault, BitLocker, or equivalent)
  - Screen lock enforced with timeout
  - Operating system and security patches kept reasonably current
  - Anti-malware protections enabled where available for the platform
- Personal devices meeting the baseline are acceptable. Personal devices that do not meet the baseline must not be used for customer data access. Public or shared devices (hotel business centers, etc.) must not be used at all.
- Devices used to access customer data must not be left unattended in unsecured locations.

7. Communication channels

Approved channels for SendTax business communication:

- **Gmail (Google Workspace)** — email
- **Google Chat** — internal messaging

- **Google Meet** — video conferencing
- **GitHub, Linear, Notion** (and other approved tools) — work coordination

These channels provide encryption in transit and at rest through Google Workspace's SOC 2 Type II / ISO 27001-certified infrastructure.

7.1 What may be communicated where

- **Customer-identifying personal data, credentials, full customer documents:** approved company channels only. Never over personal email, iMessage, SMS, social media, or any personal channel.
- **General product discussion that does not expose customer data** (architecture, roadmap, internal coordination): approved and vetted company channels.
- **Public information** (marketing, blog posts, this policy): any channel.

7.2 Data minimization

Even within approved channels, personnel apply data minimization: send only the data needed to accomplish the task. Each additional copy of a customer document in a chat, email, or attachment expands SendTax's blast radius in the event of an account compromise. When in doubt, link to the source in the application rather than copy data into a message.

8. AI tools

Personnel may use AI tools (Claude, ChatGPT, GitHub Copilot, Claude Code, and similar) to assist with their work, subject to the following restrictions:

8.1 What may be sent to AI tools

- Public information
- SendTax-owned non-confidential content (e.g., this policy text, public marketing copy)
- Code that does not include production secrets, customer data, or personally identifying information
- Architectural and process questions about SendTax that do not reveal customer-specific details

8.2 What must not be sent to AI tools

- Customer documents (tax forms, identity documents, financial records)
- Customer personally identifying information (names, SSNs, addresses, account numbers)
- Production secrets (API keys, database credentials, KMS material, JWT signing keys)
- Internal credentials of any kind
- Source code containing embedded secrets or hardcoded customer data

8.3 Responsibility for output

Personnel are responsible for the output of their work regardless of whether AI tools assisted in producing it. This includes:

- Reviewing AI output for accuracy before relying on it (AI tools can produce plausible-sounding but incorrect information)
- Verifying any factual claims, code, or recommendations against authoritative sources
- Disclosing AI assistance in contexts where it materially affected the output, where disclosure is reasonable (e.g., AI-drafted customer communications should be reviewed and edited before sending)

8.4 Approved AI tools

The current list of explicitly approved AI tools is maintained internally. Use of AI tools not on the approved list with SendTax data requires approval under the exception process in §13.

9. Account and credential handling

- Each person uses their own individual account on every system. No shared accounts, no shared passwords.
- Passwords are stored in 1Password, not in browsers, plaintext files, sticky notes, or personal password managers.
- MFA must be enabled on every system that supports it, including each system named in the **Access Control Policy** §5.1.
- Compromised or suspected-compromised credentials must be reported immediately to security@send.tax and rotated as part of incident response.

10. Tax data — IRC §7216 obligations

Personnel handling tax return information are agents of a tax return preparer for purposes of IRC §7216. This means:

- Tax return information may be used only for tax return preparation, the auxiliary services SendTax provides, and the specific purposes authorized by §7216
- Tax return information must not be disclosed to any unauthorized party or used for any unauthorized purpose
- Cross-border disclosure of tax return information without §7216-compliant consent is prohibited (SendTax operates U.S.-only and does not currently use cross-border consent mechanisms)

Violations of §7216 carry civil and potentially criminal penalties under federal law in addition to any consequences SendTax imposes.

11. Monitoring

SendTax may monitor use of company systems for security, compliance, and operational purposes. This includes review of system logs, audit logs, authentication events, application activity, and infrastructure logs. Personnel should not have an expectation of privacy in their use of company-issued accounts and systems.

Monitoring is conducted in service of security and operational integrity, not for surveillance of personal communications. Personnel personal device contents are not monitored even when the device is used for SendTax work — only what flows through SendTax-controlled systems and accounts.

12. Reporting

Personnel must report the following promptly to security@send.tax:

- Suspected or confirmed security incidents (see **Incident Response Policy**)
- Lost or stolen devices with SendTax access
- Compromised or suspected-compromised credentials
- Suspicious emails, messages, or contact attempts targeting SendTax personnel

- Violations of this policy by any person
- Operational concerns that may indicate a control gap

Reports made in good faith are protected. SendTax does not retaliate against personnel who report in good faith, even where the reported activity turns out to be benign or attributable to the reporter themselves.

13. Exceptions

A deviation from this policy may be authorized only when:

1. The deviation is documented in writing with a specific business need
2. A second SendTax operator approves the deviation
3. A defined re-evaluation point is set
4. Compensating controls are in place where the deviation reduces an existing safeguard

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

14. Enforcement

Violations of this policy may result in:

- Revocation of access to SendTax systems
- Termination of employment, contract, or engagement
- Civil or criminal referral where applicable, including for violations involving customer data, IRC §7216, or unauthorized access to taxpayer information

The consequences applied to a violation are proportional to the severity, the intent, and any pattern of prior violations. SendTax follows a blameless approach to honest mistakes that are promptly reported and remediated, consistent with the postmortem culture described in the **Incident Response Policy**.

15. Related policies

- **Information Security Policy** — umbrella security commitments

- **Access Control Policy** — what personnel access is granted, reviewed, and revoked
- **Encryption Policy** — encryption standards personnel must follow
- **Incident Response Policy** — how personnel respond to and report incidents
- **Data Retention & Deletion Policy** — handling and disposal of customer data
- **Vendor Management Policy** — personnel obligations in vendor interactions

16. Document control

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

17. Contact

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