

Written Information Security Plan

Sample Tax & Bookkeeping LLC

123 Main St, Austin, TX 78701

Effective date	November 1, 2026
Next review date	November 1, 2027
Data Security Coordinator	Pat Rivera, Owner, EA
Version	1.0

Prepared with WispMint. This plan is structured on IRS Publication 5708, IRS Publication 4557 and the elements of the FTC Safeguards Rule (16 CFR Part 314).

1. Purpose and scope

Sample Tax & Bookkeeping LLC (the "Firm") provides tax preparation and bookkeeping or payroll and therefore handles personally identifiable information (PII) and taxpayer data for its clients. As a tax and accounting practice, the Firm is a financial institution under the Gramm-Leach-Bliley Act and is required by the FTC Safeguards Rule to maintain a written information security program.

This plan sets out the administrative, technical and physical safeguards the Firm uses to protect client information. It applies to every owner, employee, contractor and seasonal worker, at its office and wherever Firm work is performed, including home offices and laptops used outside the office.

2. Objectives

1. Ensure the security and confidentiality of client PII and taxpayer data.
2. Protect against anticipated threats or hazards to that information.
3. Protect against unauthorized access to or use of that information that could result in substantial harm or inconvenience to any client.
4. Meet the Firm's obligations under the FTC Safeguards Rule, IRS Publications 4557 and 5708, and applicable state law.

3. Data Security Coordinator

Pat Rivera, Owner, EA, is the Firm's Data Security Coordinator and is responsible for implementing, maintaining and annually reviewing this plan, training staff, overseeing service providers and leading the

response to any security incident. The Coordinator may delegate tasks but remains accountable for the program.

4. Information covered by this plan

This plan covers all client information in any form, including names, addresses, dates of birth, Social Security numbers, EINs, bank account numbers, income and financial records, tax returns and supporting documents, and any IRS, state or e-Services credentials, whether held on paper or electronically.

System	Used for	Where
Drake	Return preparation and e-filing	Installed or vendor cloud
Microsoft 365 / Outlook	Client correspondence	Cloud
Office computers, a client portal or industry app and paper files	File storage	As listed
A secure portal or online forms and email attachments	Client document intake	As listed
Paper files	Source documents and records	123 Main St, Austin, TX 78701, locked storage

5. Risk assessment

The Coordinator assesses risks to client information at least annually and whenever the Firm changes software, storage, staffing or location. The assessment considers employee training and management; information systems, including network, software, storage, transmission and disposal; and the detection of and response to attacks and system failures.

The Firm is a practice of 3 to 5 people that uses Drake for return preparation, Microsoft 365 / Outlook for email, and stores files using office computers, a client portal or industry app and paper files.

For a practice of this size and setup, the most likely risks are phishing and account takeover against Microsoft 365 / Outlook and tax software logins, a lost or stolen laptop used outside the office, ransomware or hardware failure without a reliable backup, client information sent by plain email or text and paper files left out or thrown away unshredded. This plan addresses them through multi-factor authentication and access control (Section 6), device, network and backup safeguards (Section 7), physical safeguards and disposal (Section 8), and a written incident response plan (Section 10). Any safeguard not yet fully in place appears in the gap list in Section 11 with an owner and a due date.

Current status from the most recent assessment:

Area	Status	Action
------	--------	--------

Email MFA	In place	Maintain
Tax software and e-Services MFA	Verify	See Section 11
Device encryption	In place	Maintain
Backups	Verify	See Section 11
Endpoint protection	In place	Maintain
Automatic updates	In place	Maintain
Wi-Fi security	Not in place	See Section 11
Password manager	Not in place	See Section 11
Secure disposal	Not in place	See Section 11
Staff training	Not in place	See Section 11
Hiring checks	In place	Maintain

6. Administrative safeguards

6.1 Staff responsibilities. Every person with access to client information must read this plan, sign the acknowledgment in Appendix A, and complete security awareness training on hire and annually.

6.2 Hiring and departure. The Firm checks references or backgrounds for new hires with access to personal information. When anyone leaves, their accounts, keys and access are removed on their last day and Firm devices are returned.

6.3 Access control. Access to client information is limited to those who need it for their work. Each person uses their own named account; shared logins are not permitted. Passwords must be at least 12 characters, unique for each system, and never written down near the computer. The Firm will adopt a password manager by December 1, 2026.

6.4 Multi-factor authentication. MFA is required on email, tax software, IRS e-Services, cloud storage and remote access. MFA is in place on email. The Coordinator will confirm MFA is on for tax software and IRS e-Services by November 8, 2026.

6.5 Service providers. The Firm uses the service providers listed in Appendix C. Before using a provider that stores or processes personal information, the Coordinator confirms the provider offers appropriate safeguards (encryption, MFA, published security practices) and keeps a record. Providers are reviewed at the annual plan review.

6.6 Client communication. Sensitive documents are exchanged through the Firm's secure portal or online forms. Staff do not send Social Security numbers, bank details or complete returns by unencrypted email or text, and ask clients to use a secure method instead.

6.7 Annual review. The Coordinator reviews and updates this plan every year, after any security incident, and after material changes to the business. Each review is recorded in Appendix D.

7. Technical safeguards

7.1 Devices. All Firm computers run a supported operating system with automatic updates turned on, a screen lock after 10 minutes, and the operating system's built-in protection (Microsoft Defender or macOS security) kept on and current. Full-disk encryption (BitLocker or FileVault) is turned on.

7.2 Network. By December 1, 2026, Wi-Fi will use a strong password, guests will use a separate network, and the router's default admin password will be changed. Remote work is done only on Firm devices with encryption on, over a secured home network or a VPN, and never on public Wi-Fi without a VPN.

7.3 Data storage and transmission. Files are stored using office computers, a client portal or industry app and paper files. Data is encrypted in transit (HTTPS/TLS) and at rest where the platform supports it. Client information is not stored on personal devices, USB drives or personal cloud accounts.

7.4 Backups. Backups are made to an encrypted external drive at least weekly and stored securely. The Firm will add an automatic offsite backup by December 1, 2026.

7.5 Monitoring. The Coordinator reviews sign-in alerts and unusual activity notices from Microsoft 365 / Outlook, Drake and IRS e-Services, and checks the e-file "returns filed" count in IRS e-Services weekly during filing season.

8. Physical safeguards

Paper files containing personal information are kept in locked cabinets or a locked room when not in use. Desks are cleared of sensitive documents at the end of the day. Visitors do not have unescorted access to work areas, and screens are positioned so that visitors cannot read client data. Beginning immediately, paper is cross-cut shredded and retired drives are wiped or destroyed. The Firm will obtain a shredder or shredding service by November 15, 2026.

9. Data retention and disposal

Client records are kept for the period required by IRS rules and state law (generally at least three years from the return due date or filing date, and longer where required), then destroyed as described in Section 8. The Firm keeps only the information it needs.

10. Incident response plan

An incident is any suspected or confirmed unauthorized access to, loss of, or misuse of personal information, including a lost or stolen device, a compromised email account, a ransomware infection, or a suspicious IRS or e-file notice.

1. Contain. Disconnect affected devices from the network. Change passwords and sign out all sessions on affected accounts. Do not wipe or power off devices that may be needed for investigation.

2. **Notify the Coordinator** immediately: Pat Rivera, Owner, EA, (555) 555-0100.
3. **Report to the IRS.** Contact the IRS Stakeholder Liaison for TX and follow the data theft guidance in IRS Publication 4557.
4. **Report to the FTC** within 30 days of discovery if the incident involves the unencrypted information of 500 or more consumers, as the Safeguards Rule requires.
5. **Notify state authorities and clients** as required by TX breach notification law and the law of any other state whose residents are affected.
6. **Notify** the Firm's cyber insurer, its tax software vendor, and law enforcement where appropriate.
7. **Recover** from backups, confirm systems are clean, and restore normal operation.
8. **Record** the incident and the response in Appendix D, and update this plan within 30 days.

11. Gap list and action items

#	Gap	Action	Owner	Due
1	Secure disposal (not in place)	Get a cross-cut shredder or shredding service and wipe or destroy retired drives.	Pat Rivera, Owner, EA	November 15, 2026
2	Wi-Fi security (not in place)	Use a strong Wi-Fi password, move guests to a separate network, and change the router's admin password.	Pat Rivera, Owner, EA	December 1, 2026
3	Password manager (not in place)	Adopt a password manager and give every person unique passwords of 12+ characters.	Pat Rivera, Owner, EA	December 1, 2026
4	Staff training (not in place)	Complete security awareness training for everyone and record the date.	Pat Rivera, Owner, EA	December 31, 2026
5	Tax software and e-Services MFA (verify)	Confirm status. If not in place: Turn on MFA in your tax software and confirm it on IRS e-Services for every user.	Pat Rivera, Owner, EA	November 8, 2026
6	Backups (verify)	Confirm status. If not in place: Set up automatic, encrypted offsite backups and test a restore.	Pat Rivera, Owner, EA	November 15, 2026

Appendix A. Employee acknowledgment

I have read and understand the Sample Tax & Bookkeeping LLC Written Information Security Plan and agree to follow it.

Name: _____ Signature: _____ Date: _____

Name: _____ Signature: _____ Date: _____

Name: _____ Signature: _____ Date: _____

Name: _____ Signature: _____ Date: _____

One line per person. Add pages as needed.

Appendix B. Security awareness training checklist (annual)

- Recognizing phishing emails and texts, including fake IRS and software-vendor messages
- Using MFA and the password manager
- Handling client documents: secure method first, never SSNs by plain email
- Locking screens, clean desk, shredding
- Reporting an incident right away, with no blame
- Review of this year's plan changes

Appendix C. Service provider list

Provider	Service	Holds personal data?	Safeguards confirmed	Date reviewed
Drake	Tax software	Yes		
Microsoft 365 / Outlook	Email	Yes		
Cloud storage / portal	File storage	Yes		

Appendix D. Review and incident log

Date	Event	Summary	Signed
November 1, 2026	Plan adopted	Version 1.0	Pat Rivera

Appendix E. Key contacts

Contact	Details
Data Security Coordinator	Pat Rivera, Owner, EA, (555) 555-0100
IRS Stakeholder Liaison, TX	irs.gov, search "Stakeholder Liaison local contacts"
IRS Identity Protection Specialized Unit	800-908-4490
FTC Safeguards Rule breach notice	ftc.gov, Safeguards Rule notification form
TX Attorney General	State breach notification page
Cyber insurance carrier	_____