Written Information Security Plan (WISP)

Harbor Lane Tax & Bookkeeping (SAMPLE)
123 Example St, Suite 4, Ventura, CA 93001
Effective: November 15, 2026 · Next review due: November 15, 2027
Distribution: owner, Data Security Coordinator, all staff with access to client information. Confidential.

I. Objective

Harbor Lane Tax & Bookkeeping (SAMPLE) ("the Firm") creates this Written Information Security Plan to protect the personally identifiable information (PII) of our clients, employees and contractors, as required by the Gramm-Leach-Bliley Act and the Federal Trade Commission Safeguards Rule (16 CFR Part 314), and as expected of paid tax return preparers by the IRS. This plan is based on IRS Publication 5708 and addresses each element of 16 CFR 314.4.

II. Purpose

To ensure the security and confidentiality of client information; protect against anticipated threats to its security or integrity; and protect against unauthorized access to or use of that information that could result in substantial harm or inconvenience to any client.

III. Scope

This plan applies to all PII the Firm collects, stores, uses, transmits or disposes of, in paper or electronic form, and to all owners, employees, seasonal staff and contractors. PII includes names, addresses, Social Security and taxpayer identification numbers, dates of birth, bank and account information, income and tax return data, identity documents and any combination of data that could identify a person.

IV. Identified Responsible Officials

Role	Name	Duties
Data Security Coordinator (Qualified Individual under 16 CFR 314.4(a))	Maria Lopez, EA	Implements, oversees and enforces this plan; leads risk assessment and annual review; approves exceptions in writing; reports at least yearly to the owner; leads incident response.
Public Information Officer	Maria Lopez, EA	Sole spokesperson for the Firm after a security event; coordinates notices to clients, agencies and the media.
Principal Owner	Maria Lopez, EA, Owner	Approves this plan, accepts residual risks, receives the annual report.

If the Data Security Coordinator is a service provider or affiliate rather than an employee, the Firm remains responsible for compliance, Maria Lopez, EA oversees that person, and the provider must maintain its own information security program (16 CFR

314.4(a)).

V. Risk Assessment (16 CFR 314.4(b))

The Data Security Coordinator assessed reasonably foreseeable internal and external risks to client information as of November 15, 2026. The Firm maintains information on fewer than 5,000 consumers and is therefore exempt from the written risk assessment requirement in 314.4(b)(1); it documents this assessment as good practice.

Risk	What could happen	Current rating	Safeguards / response
Phishing / stolen passwords	Staff receive fake emails that capture logins	Medium	MFA on email and tax software; training; password manager
Ransomware	Malware encrypts files and demands payment	Medium	Endpoint protection; automatic updates; encrypted offsite backups; restore tests
Lost or stolen laptop/phone	A device with client data is lost	**High**	Full-disk encryption; screen locks; remote wipe where available
Remote access abuse	Attackers use remote tools to get in	Low	MFA on all remote access; remove unused tools
Insider misuse or departing staff	Authorized users misuse or keep access	Low	Least-access; same-day offboarding; acknowledgements; logging
Vendor / cloud provider breach	A provider holding client data is breached	Medium	Choose reputable providers; MFA; contract terms; review yearly
Physical theft or snooping	Paper or devices taken from the office	Low	Locked cabinets; office locked when unattended; visitor control
Improper disposal	Data recovered from discarded paper or drives	Low	Cross-cut shredding; secure wipe or destruction; records
Unsecured file exchange	Documents intercepted in regular email	**High**	Secure portal or encrypted email
Fraudulent returns using stolen data	Criminals file returns using client identities	Medium	Watch EFIN activity; IP PINs for clients; incident plan

Criteria: High = likely and harmful with current controls; Medium = possible, with partial controls; Low = controls in place. C/I/A = confidentiality, integrity, availability. Decision: Mitigate unless the owner accepts or transfers (insures) the risk in writing below. Re-rate at every annual review and after any material change.

VI. Inside the Firm Risk Mitigation

PII Collection and Retention Policy

The Firm collects only the PII needed to prepare returns and provide services. PII is stored only in: Drake Tax (Installed on our computers); Paper files; Client portal; Cloud storage. Named services: SmartVault portal; Microsoft 365. **Email is not an approved place to store PII; PII found in mailboxes is moved to approved storage and deleted (action item).** A list of systems and devices holding PII is kept in Attachment E.

Client records are retained for **7 years** after the last engagement because: The IRS assessment period can extend to 6 years for substantial omissions (IRC 6501(e)); records are kept to support client examinations, amended returns and state inquiries. Records past that period are destroyed securely (see Attachment A). Retention is reviewed at each annual review.

Personnel Accountability Policy

- Access to PII is limited to the people listed in Attachment F, and only to the data they need.
- New staff are screened before access is granted and **will sign** the acknowledgement in Attachment D.
- When anyone leaves, the Data Security Coordinator disables accounts, changes shared passwords, and collects keys, badges and devices the same day. A secured master list of accounts, keys and combinations is kept by the Coordinator.
- Violations of this plan may result in discipline up to termination.

PII Disclosure Policy

PII is shared only with the client, the IRS and state tax agencies, and service providers needed to deliver services (see Service Providers below), or as required by law. Staff verify a caller's identity before discussing any client information, and never send PII to an unverified email address or phone number.

Reportable Event Policy

Any staff member who suspects that PII has been lost, stolen, accessed or disclosed without authorization reports it immediately to the Data Security Coordinator. The Firm then follows the Incident Response Plan in Attachment C.

VII. Outside the Firm Risk Mitigation (Safeguards, 16 CFR 314.4(c))

Safeguard	Firm standard	Current status
Access controls	Unique user accounts; least access; review user list at each annual review	3 person(s) listed
Data and device inventory	All systems and devices with PII listed in Attachment E	See Attachment E
Encryption	Encrypt PII at rest (full-disk encryption) and in transit (TLS, secure portal or encrypted email)	**Some — action item**

Multi-factor authentication	MFA for tax software, email, cloud services and remote access	Tax software: Yes; Email: Yes; Cloud/remote: Yes
Endpoint protection	Antivirus/endpoint protection on every computer, auto-updating	Microsoft Defender for Business
Network protection	Firewall between office and internet; default passwords changed	In place
Patching	Automatic updates for operating systems, browsers and tax software	In place
Passwords	Unique passwords of 14+ characters; password manager; never shared	**Action item**
Backups	Automatic, encrypted, offsite; restore tested yearly	Yes, automatically to cloud or offsite, encrypted; restore tested: **No**
Wi-Fi access	WPA2/WPA3, strong password, separate guest network	WPA2/WPA3 with a strong password and a separate guest network
Remote access	Only through approved tools with MFA	Remote access tool with MFA
Connected and personal devices	Only approved devices; screen lock, encryption, updates and MFA required	Personal devices used: No
Electronic exchange of PII	Secure portal or encrypted email only; no PII in regular email	**Secure client portal; Regular email; In person / paper**
Secure disposal	Paper: Shredding service with certificate. Electronic: Wiped with a secure-erase tool or physically destroyed	Destroyed when the 7-year retention period ends (see Attachment A)
Secure development and applications	The Firm does not develop software in-house. Third-party applications that handle PII are evaluated (MFA, encryption, vendor security) before adoption under change management (16 CFR 314.4(c)(4))	Adopted with this plan
Change management	New software, devices or vendors that touch PII are approved by the Data Security Coordinator before use and added to Attachment E	Adopted with this plan
Monitoring and logging	Login, antivirus and email alerts reviewed at least weekly	We review alerts from our antivirus/email ourselves
Physical security	Paper and equipment locked when unattended; visitors escorted	In place

Interim compensating controls (approved by the Data Security Coordinator)

Until the related action items are completed, the following interim controls apply under 16 CFR 314.4(c)(3) and (c)(5):

Gap	Interim control	Target date
Not all devices encrypted	Unencrypted devices hold no client PII (work from encrypted devices or the tax software only); unencrypted devices do not leave the office	_____
Clients send documents by regular email	Clients are asked to use the portal; emailed PII is saved to approved storage and deleted from the mailbox within 1 business day; no PII is sent out by regular email	_____

Maria Lopez, EA, Data Security Coordinator — approves

Date

Any exception to MFA or encryption must be approved in writing by the Data Security Coordinator with an equivalent compensating control, as allowed by 16 CFR 314.4(c)(3) and (c)(5).

Information Security Training Policy (16 CFR 314.4(e))

Everyone with access to PII completes security awareness training when hired and at least once a year, using the Firm’s training handout, and signs the acknowledgement in Attachment D. Current practice: Only when hired. The Data Security Coordinator keeps their own knowledge current through IRS, FTC and professional guidance.

Testing and Monitoring (16 CFR 314.4(d))

The Data Security Coordinator checks key safeguards at least yearly: MFA on all accounts, encryption on all devices, updates current, backups restorable, user list correct. As a firm with fewer than 5,000 consumers, the Firm is exempt from the annual penetration test and six-monthly vulnerability scan in 314.4(d)(2), but will perform them if it grows past that threshold. Additional checks follow any material change.

Service Providers (16 CFR 314.4(f))

The Firm uses only service providers that can protect client information (including: Drake Tax (tax software); SmartVault portal; Microsoft 365; shredding service; backup provider; Microsoft Defender for Business (endpoint protection)). Contracts or terms of service must require them to safeguard PII. Providers are reviewed at each annual review.

Program Updates (16 CFR 314.4(g))

This plan is reviewed and updated at least annually (next review due November 15, 2027), and after any security event, material change in operations, new system, or change in law.

Annual Report (16 CFR 314.4(i))

At least yearly the Data Security Coordinator gives the owner a written report on the plan’s status, risks, test results, security events and recommended changes, using the Annual Report form provided with this plan. (Exempt for firms under 5,000 consumers; adopted as good practice.)

VIII. Implementation

This plan is effective November 15, 2026.

Maria Lopez, EA, Owner Date

Maria Lopez, EA, Data Security Coordinator Date

Prepared with a template tool from the Firm’s own answers. Not legal advice; does not certify compliance. The Firm is responsible for the accuracy of its answers and for carrying out this plan.

Attachments to the WISP

Harbor Lane Tax & Bookkeeping (SAMPLE) · Effective November 15, 2026

Attachment A — Record Retention and Disposal

Record type	Retention	Disposal method
Client tax returns, workpapers and source documents	7 years after last engagement	Paper: Shredding service with certificate. Electronic: secure deletion from all systems and backups as they age out
List or copies of returns prepared (IRC 6107)	At least 3 years after the close of the return period	As above
Form 8879 / 8878 e-file authorizations	3 years from the later of the return due date or the date the IRS received the return (IRS Pub 1345)	As above
Engagement letters	Firm policy: 7 years after last engagement	As above
Retired computers, drives, copiers, phones	Until disposal	Wiped with a secure-erase tool or physically destroyed; record serial number, date and method

Reason for retention beyond two years after last use: The IRS assessment period can extend to 6 years for substantial omissions (IRC 6501(e)); records are kept to support client examinations, amended returns and state inquiries.

Attachment B — Rules of Behavior for Safeguarding Client PII

1. Access only the client information you need for your job.
2. Use your own account; never share passwords or MFA codes. Use the password manager.
3. Lock your screen when you step away (Windows + L / Control + Command + Q).
4. Never email Social Security numbers or tax documents in regular email; use the portal or encrypted email.
5. Verify identity before discussing client information by phone; call back on a number already on file.
6. Treat unexpected emails, attachments, links and “urgent” requests as suspicious. Report them to the Data Security Coordinator.
7. Do not install software or connect USB drives without approval.
8. Keep paper files in locked storage; clear your desk at the end of the day; shred, never trash, PII.
9. Use only approved devices; keep them updated, encrypted and locked.
10. Report any lost device, suspicious activity or mistake immediately — speed limits harm.

Attachment C — Security Breach Procedures and Notifications (Incident Response Plan, 16 CFR 314.4(h))

Goal: contain the incident, protect clients, meet notification duties, and restore operations. **Decision authority:** Maria Lopez, EA (Data Security Coordinator) leads; Maria Lopez, EA (Public Information Officer) handles all outside communication; Maria Lopez, EA approves notifications and spending.

Step 1 — Contain (first hour)

- Disconnect affected devices from the network (unplug cable / turn off Wi-Fi). Do not wipe or turn off unless instructed — evidence matters.
- Change passwords for affected accounts from a clean device; sign out all sessions; confirm MFA.
- Call the IT contact and the cyber insurer's breach hotline before hiring anyone (insurers often require their own vendors).

Step 2 — Assess (first 24 hours)

- What happened, when, which systems, which clients, what data (SSNs, bank data, returns)?
- Was data encrypted? Is it still happening? Start an incident log (time, action, person).

Step 3 — Notify

Who	When	Contact
Cyber / liability insurer	Immediately	_____
Attorney	Immediately	_____
IT support	Immediately	_____
IRS Stakeholder Liaison for CA	Immediately	Find yours at irs.gov — search "Stakeholder Liaison local contacts"
State tax agency (CA)	Immediately	Federation of Tax Administrators "Report a Breach" page (taxadmin.org)
State Attorney General / consumer notice	Per state law (California Civil Code 1798.82: notify residents in the most expedient time possible and without unreasonable delay; also notify the Attorney General if more than 500 California residents are notified)	State Attorney General website
FTC — if unencrypted information of 500+ consumers was acquired without authorization (or encrypted data where the key	As soon as possible and no later than 30 days after discovery. Discovery = the first day any employee or agent knows of it. Law enforcement may request a delay	Online form at ftc.gov. Include: firm name and contact, description of the types of information involved, date or date range, number of consumers affected, general description of the

was also accessed, 16 CFR 314.2(m))		event, and whether law enforcement requested a delay
Local police; FBI IC3 for cyber-crime	Promptly	_____; ic3.gov
Tax software vendor	Promptly	Drake Support (see vendor site)
Affected clients	Without unreasonable delay, as required by state law (counsel reviews the notice; review must not delay it)	Letter template from counsel/insurer; recommend IRS IP PIN and credit freeze

Step 4 — Recover and watch

- Restore from clean backups; rebuild infected devices.
- Check EFIN activity weekly for unexpected returns (especially odd hours/weekends) and e-Services accounts.
- Help clients get IRS Identity Protection PINs.

Step 5 — Document and improve

- Keep the incident log, notices sent and costs. Within 30 days, the Data Security Coordinator reviews what happened and updates this plan.

Attachment D — Employee / Contractor Acknowledgement

I have received and read the Harbor Lane Tax & Bookkeeping (SAMPLE) Written Information Security Plan and Rules of Behavior (Attachment B), completed security training, and agree to follow them. I understand that client information is confidential during and after my work with the Firm, and that violations may lead to discipline up to termination and legal action.

Name	Role	Signature	Date	Training completed
Maria Lopez	Owner / preparer			
James Park	Preparer			
Dana Reyes	Seasonal assistant (Jan-Apr)			

Attachment E — Hardware, Systems and Services Containing PII

Item / system	Product or provider	Location / type	Encrypted? MFA?
Tax software	Drake Tax	Installed on our computers	MFA: Yes

Paper files			
Email (not approved for PII storage)			
Client portal			
Cloud storage			
Named cloud / portal services	SmartVault portal; Microsoft 365	Cloud	MFA: Yes

Add every computer, laptop, phone, tablet, server/NAS, external drive, copier with storage, and cloud service. Update when anything is added or retired (change management).

Attachment F — People Authorized to Access PII

Name	Role	PII access	Systems	Access granted	Access removed
Maria Lopez	Owner / preparer	Yes			
James Park	Preparer	Yes			
Dana Reyes	Seasonal assistant (Jan-Apr)	Yes			

Security Action Plan

Harbor Lane Tax & Bookkeeping (SAMPLE) · Prepared November 15, 2026 · Items found from your answers

Your answers show **8** item(s) to fix. Fix High items within 30 days, Medium within 90 days, Low within the year. Record completion dates; the next annual review checks them.

#	Priority	Action	How to fix	Basis	Done (date)
1	**High**	Encrypt all computers and laptops	Turn on BitLocker (Windows Pro), Device Encryption (Windows Home) or FileVault (Mac) on every device that stores client data; store recovery keys securely; replace devices that support neither.	FTC 314.4(c)(3)	
2	**High**	Stop receiving tax documents by regular email	Move clients to a secure portal or encrypted email; tell clients not to email SSNs or tax documents. Until then, use the interim controls in Section VII.	FTC 314.4(c)(3); IRS Pub 5708 Electronic Exchange of PII	
3	Medium	Use a password manager and unique passwords	Adopt a business password manager; require unique passwords (firm standard: at least 14 characters, per NIST SP 800-63B guidance).	IRS Pub 4557 (strong passwords); NIST SP 800-63B	
4	Medium	Test restoring from backup	Restore a sample of files at least once a year and record the date in the annual report.	FTC 314.4(d)(1)	
5	Medium	Train everyone at least yearly	Give everyone the training handout in this plan each year and keep signed acknowledgements.	FTC 314.4(e)	
6	Medium	Move client PII out of email mailboxes	Save documents that arrive by email to approved storage and delete them from mailboxes; set a mailbox retention rule.	FTC 314.4(c)(3), (c)(6)	
7	Low	Have staff sign confidentiality agreements	Have every employee and contractor sign the acknowledgement in Attachment D.	IRS Pub 5708 Attachment D	
8	Low	Record your cyber insurance contact (or consider coverage)	Add your insurer’s breach hotline to the incident plan; if you have none, ask your agent about cyber coverage.	IRS Pub 5708 Attachment C	

Annual Security Training — Harbor Lane Tax & Bookkeeping (SAMPLE)

15-minute read · Everyone with access to client information · Sign Attachment D after completing

Why this matters

Tax preparers hold exactly what identity thieves want: names, Social Security numbers, bank accounts and income. One stolen login can lead to fraudulent returns filed in our clients' names. Federal law (the FTC Safeguards Rule) requires us to protect this information, and the IRS asks every preparer to confirm they have a security plan.

The ten habits

1. **Spot phishing.** Be suspicious of urgency, new "clients" sending attachments, password-reset emails you didn't request, and look-alike addresses. When unsure, call the sender on a known number.
2. **Never give MFA codes** to anyone, ever — including callers claiming to be IT or the IRS.
3. **Use the password manager**; one unique long password per account.
4. **Lock your screen** whenever you walk away.
5. **No PII in regular email.** Use the portal or encrypted email.
6. **Verify callers** before discussing a client; call back on the number on file.
7. **Approved devices only**; no unknown USB drives.
8. **Clean desk**; lock paper away; shred, never trash.
9. **Install updates** when prompted; don't postpone for weeks.
10. **Report fast.** Mistakes happen; hiding them makes them worse. Tell Maria Lopez, EA immediately.

Quick check (answer before signing)

1. A "client" you've never heard of emails an attachment called "W-2s.zip". What do you do? *(Don't open; verify by phone; report.)*
2. Someone calls from "IT" and asks for the code just sent to your phone. *(Refuse; hang up; report.)*
3. A client asks you to email their return. *(Use the portal or encrypted email.)*
4. You left your laptop on the train. *(Report to the Data Security Coordinator immediately.)*
5. Where do you put papers with SSNs you no longer need? *(Shredder or shred bin.)*

Annual Security Self-Review

Harbor Lane Tax & Bookkeeping (SAMPLE) · Prepared by the owner, who is also the Data Security Coordinator (the 314.4(i) report is not required for firms under 5,000 consumers; kept as good practice) · Period ending _____

Item	Status / notes
Overall status of the WISP and compliance	
Risk assessment re-rated (any new risks?)	
Action plan items completed / open	
MFA confirmed on all accounts (date checked)	
Encryption confirmed on all devices (date checked)	
Backup restore test (date, result)	
User access list reviewed; departed staff removed	
Training completed by all staff (date)	
Service providers reviewed	
Security events during the year and response	
Changes to systems, staff or operations	
Recommended changes for next year	

Maria Lopez, EA, Data Security Coordinator Date

Maria Lopez, EA, Owner (received) Date

Annual review checklist: open this tool, click “Load last year’s answers”, update anything that changed, regenerate, sign, and file this report with the new plan. Remember the IRS asks about your WISP when you renew your PTIN.

About this document. Generated by the WritAssure WISP Builder (writassure.com) from the Firm's own answers, based on the FTC Safeguards Rule (16 CFR Part 314), IRS Publication 5708 (Rev. 8-2024) and IRS Publication 4557. It is a template tool, not legal advice, and does not certify compliance. The Firm is responsible for the accuracy of its answers and for carrying out this plan. Consult an attorney for legal questions and state-specific breach-notification duties.