

Written Information Security Plan

TEMPLATE FOR TAX & ACCOUNTING PRACTICES

EDITABLE • FILLABLE • 2026 PROFESSIONAL EDITION

A practical operating document for U.S. tax preparers, bookkeepers and accounting firms.
Complete every prompt, assign each action and retain evidence of implementation.

USE THIS TEMPLATE TO

01

Map exposure

Document information, systems, access and vendors.

02

Assign controls

Give safeguards, risks and open actions clear owners.

03

Retain evidence

Create an approval, testing and review trail.

BASED ON CURRENT GUIDANCE FROM

FTC Safeguards Rule | IRS Publications 4557 and 5708

Version 2.0 • Last reviewed October 2026

Prepared by the Small Business Insured Editorial Team

smallbusinessinsured.com | admin@smallbusinessinsured.com

Independent educational template — not an official IRS form and not legal, cybersecurity, tax or insurance advice.

Begin here, then work through the plan in order.

Before you type

Save a controlled working copy, appoint one owner and collect current system, vendor, insurance and incident-contact information.

1. Scope: Confirm the practices, people, systems and customer information covered by this plan.
2. Assess: Inventory data and tools, rate risks and record current safeguards and gaps.
3. Act: Give each open item an owner, due date and evidence source.
4. Approve: Obtain qualified review where appropriate, secure leadership approval and train personnel.
5. Maintain: Test safeguards, review vendors and update the WISP after material change and at least annually.

Document map

Each section is designed as a one-page working module.

PAGES	MODULE	PAGES	MODULE
3	Applicability and use	11	Vendor oversight
4	Profile and governance	12	Training, monitoring and testing
5–6	Information and tool inventory	13–14	Incident response and reporting
7	Written risk assessment	15	Continuity, retention and disposal
8	Core safeguards	16	Annual report and change control
9	Access, devices and remote work	17	Suggested 30-day implementation
10	Personnel accountability	18–19	Glossary, sources and notice

Completion standard: A bracketed prompt is unfinished. Replace it with a fact, decision, responsible person, date or documented “not applicable” rationale.

Document why the program fits the practice; do not assume that small means exempt.

A template is not a completed security program

The written program should fit the size and complexity of the practice, the nature and scope of its activities and the sensitivity of the customer information it handles. Adapt this document to actual operations and retain evidence that safeguards work.

Applicability screen

Record the facts used to determine the practice's obligations.

Customer information maintained	
Estimated consumers represented	
Fewer than 5,000 consumers	
Applicable federal requirements	
Applicable state / contractual duties	
Assessment completed by / date	

Small-institution point: Maintaining customer information concerning fewer than 5,000 consumers may exempt a financial institution from certain enhanced Safeguards Rule provisions; it does not remove the rule or every safeguard obligation. Confirm the effect for this practice with qualified counsel.

Use and evidence rules

Apply these rules throughout the document.

- ☐ Replace every prompt; do not leave silent blanks.
- ☐ Link every material safeguard to an owner, review frequency and evidence source.
- ☐ Mark an item not applicable only with a short documented rationale.
- ☐ Keep sensitive security details in a restricted appendix if broad distribution creates risk.
- ☐ Review after incidents, major system or vendor changes, staffing changes and new legal obligations.

Define the business context, authority and approval path.

Practice profile

Complete the snapshot before selecting or evaluating safeguards.

Practice legal name	
Locations and remote-work model	
Personnel and seasonality	
Services and annual return volume	
Critical systems	
Cyber / professional insurance	

Governance assignments

Authority must be explicit enough to support decisions and escalation.

ROLE	NAMED PERSON	CORE RESPONSIBILITY	BACKUP
Qualified Individual		Direct, enforce and report on the program	
Practice leader		Approve resources, risk decisions and annual report	
Incident lead		Coordinate response, counsel, insurer and reporting	
Technology lead		Operate, monitor and evidence technical safeguards	
Privacy / records lead		Oversee retention, disposal and client communications	

Approval record: Version [enter version] approved by [name / body] on [date]. Next scheduled review: [date].

Controlled copy location: [secure location].

Map sensitive information from collection through disposal.

Information register

Record where information originates, where it moves and who can reach it.

INFORMATION / PROCESS	SOURCE	SYSTEM / LOCATION	ACCESS	RETENTION / DISPOSAL
Taxpayer identity and return data				
Banking and payment details				
Payroll and employee records				
Identity documents and e-signatures				
Client communications and attachments				
Backups, exports and temporary files				

Data-flow checkpoints

For each material workflow, confirm the following.

- ☐ Collection uses a secure portal or approved transfer method rather than ordinary email where feasible.
- ☐ The practice can identify every authorized recipient, integration and downstream copy.
- ☐ Downloads, exports, printouts and removable media are restricted and disposed of securely.
- ☐ Retention is tied to legal, business and contractual need rather than indefinite convenience.
- ☐ Backups and archives have access controls, encryption and tested restoration procedures.

Deliverable: Attach a simple data-flow diagram if a workflow crosses multiple systems or service providers.

Include convenience tools that can quietly copy, retain or expose customer information.

Technology register

Inventory sanctioned and unsanctioned tools, including trial and seasonal use.

TOOL CATEGORY	PRODUCT / OWNER	CUSTOMER DATA USED	APPROVED?	KEY CONTROL / REVIEW
Tax, bookkeeping and payroll				
Portal, e-signature and file sharing				
Email, messaging and video				
AI assistants and copilots				
OCR, scanning and transcription				
Browser extensions and automations				
Personal devices or cloud storage				

Minimum approval questions

Answer before customer information enters a new tool.

- ☐ Is customer information used to train a model, retained after use or accessible to provider personnel?
- ☐ Are encryption, MFA, logging, deletion, incident notice and subcontractor terms adequate?
- ☐ Can the practice export information and revoke all access when the service ends?
- ☐ Has the Qualified Individual approved the use case and prohibited unsafe uses in writing?
- ☐ Can the practice monitor actual use rather than relying only on policy language?

Use a consistent method and connect every high risk to action.

Rating method

Score Likelihood from 1 (rare) to 5 (almost certain) and Impact from 1 (limited) to 5 (severe). Risk score = Likelihood × Impact.

SCORE	RATING	EXPECTED RESPONSE
1–5	Low	Maintain controls; review on schedule.
6–14	Moderate	Plan improvement; assign owner and date.
15–25	High	Escalate promptly; reduce, avoid, transfer or formally accept.

Risk register

Describe the real scenario and evaluate remaining risk after current safeguards.

RISK SCENARIO / ASSET	L	I	SCORE	CURRENT SAFEGUARDS	ACTION / OWNER / DUE
Phishing or mailbox takeover					
Stolen or compromised credentials					
Ransomware or destructive malware					
Lost device or insecure remote work					
Vendor or integration compromise					
Improper access, export or disposal					

Decision record: Any accepted moderate or high residual risk requires [approver], [rationale], [review date] and [monitoring evidence].

Describe what is implemented, not what the practice merely intends to do.

SAFEGUARD	PRACTICE STANDARD	OWNER	FREQUENCY	EVIDENCE / STATUS
MFA	Required for email, tax, portal, storage, remote access and administration		Continuous	
Encryption	Protect customer information in transit and at rest or document an approved alternative		Annual / change	
Secure configuration	Approved settings, supported software, patching and prohibited services		Monthly	
Endpoint protection	Managed anti-malware, firewall, device encryption and screen lock		Continuous	
Backups	Protected, separated backups with documented restoration tests			
Logging and alerting	Monitor critical systems, privileged activity and security events			
Change management	Review material changes before deployment and verify controls afterward		Per change	
Secure disposal	Destroy data and media so information cannot practicably be read or reconstructed		Per schedule	

Open safeguard decisions

Record the next three priority improvements.

PRIORITY ACTION	RISK ADDRESSED	OWNER	DUE	SUCCESS EVIDENCE

Reduce standing access and make every device and account accountable.

Access standard

Document rules that can be tested through account lists, settings and logs.

- ☐ Each person uses a unique account; shared credentials are prohibited or formally controlled.
- ☐ Access is role-based, approved before use and reviewed at least every [frequency].
- ☐ Privileged accounts are separate from ordinary work and protected by phishing-resistant MFA where feasible.
- ☐ Departing and seasonal personnel lose access promptly through a documented offboarding checklist.
- ☐ Password managers, recovery methods and emergency access are approved and securely maintained.
- ☐ Remote access uses approved devices, secure connections and restricted local storage and printing.

Account and device review

Use this register for high-risk systems and endpoints.

SYSTEM / DEVICE GROUP	OWNER	MFA / ENCRYPTION	LAST ACCESS REVIEW	NEXT ACTION
Email and identity platform				
Tax and accounting applications				
Client portal and e-signature				
Workstations and mobile devices				
Remote support and administrator tools				

Exception process: Exception approved by [name] on [date], business reason [reason], compensating control [control], expiration [date].

Set expectations before access begins and document acceptance.

Personnel controls

Apply controls proportionate to role, access and applicable law.

- ☐ Screen candidates and contractors where lawful and appropriate to the role.
- ☐ Use confidentiality, acceptable-use, remote-work and incident-reporting obligations.
- ☐ Grant access only after required training and signed acknowledgment.
- ☐ Supervise seasonal and temporary personnel and remove access at the end of the engagement.
- ☐ Apply a documented disciplinary process for deliberate or repeated violations.
- ☐ Recover devices, records, credentials and keys during role change or separation.

Employee / contractor acknowledgment

Retain one signed copy for each person with access to customer information.

I acknowledge that I received and understand the practice's information-security policies and training. I will use customer information only for authorized work, follow approved safeguards, protect credentials and devices, and report suspected loss, misuse, phishing, malware, unauthorized access or disclosure immediately through the stated reporting channel. I understand that violations may result in loss of access or disciplinary action, subject to applicable law and policy.

Name and role	
Signature	
Date	
Manager / witness	
Training completed	

Immediate reporting channel: [Enter phone, secure email and backup contact]. Personnel should not investigate or erase evidence unless directed by the incident lead.

Apply deeper review when a provider can reach sensitive systems or customer information.

PROVIDER / SERVICE	DATA / ACCESS	RISK	DUE DILIGENCE	CONTRACT / INCIDENT TERMS	REVIEW

Risk-based review

Confirm and retain evidence appropriate to the provider's access and criticality.

- ☐ Security program, independent assurance, encryption, MFA, logging and vulnerability management.
- ☐ Data location, retention, deletion, subcontractors, model training and secondary use.
- ☐ Incident-notice timing, cooperation, investigation records and allocation of responsibility.
- ☐ Business continuity, backup, recovery targets, financial viability and exit support.
- ☐ Contractual safeguards, confidentiality, audit rights and cyber-insurance requirements.
- ☐ Termination steps: export, verified deletion, access revocation and integration cleanup.

Review cadence: High-risk providers [frequency]; other providers [frequency]; all material changes and incidents [trigger].

Measure behavior and control performance, not just attendance.

Operating schedule

Set a cadence the practice can evidence throughout the year.

ACTIVITY	AUDIENCE / SCOPE	FREQUENCY	OWNER	EVIDENCE / LAST RESULT
Security awareness and tax-scam training	All personnel	Hire + annual + seasonal		
Phishing exercise or equivalent check	Email users			
Access and privileged-role review	Critical systems			
Vulnerability / patch review	Managed devices and systems			
Backup restoration test	Critical data and systems			
Incident tabletop exercise	Response team	At least annual		
Program effectiveness review	WISP safeguards	At least annual		

Metrics for leadership

Select a small set that exposes delay or control failure.

- MFA coverage, unsupported devices, critical patch age and unresolved high risks.
- Training completion, repeat simulation failures and time to remove departing-user access.
- Backup success and restoration time, vendor reviews overdue and incident-response actions open.

Current reporting cadence	
Issue escalation threshold	
Evidence repository	

Protect people and evidence, contain safely and coordinate required notifications.

Report suspected tax-practice data theft immediately

Contact the IRS Stakeholder Liaison for the practice's state or territory as soon as suspected client data theft is identified. Also follow insurer, legal, law-enforcement and state reporting procedures applicable to the facts.

First-response sequence

The incident lead adapts the sequence to the event; safety and legal direction take priority.

1. Escalate: Use the offline contact sheet; involve the Qualified Individual, technology lead, counsel and insurer as appropriate.
2. Preserve: Record who discovered what and when; preserve messages, logs, devices and timelines. Do not destroy or casually alter evidence.
3. Contain: Isolate affected accounts or systems, revoke sessions and block malicious activity under technical and legal direction.
4. Assess: Identify systems, information, people, dates and jurisdictions affected; distinguish confirmed facts from assumptions.
5. Notify: Apply the reporting matrix and policy notice terms; coordinate communications so they are accurate and authorized.
6. Recover and learn: Restore safely, monitor for recurrence, document decisions and update safeguards after the event.

Warning signs

Treat these as potential incidents until reviewed.

- Unexpected e-file rejections, client transcripts, account changes or preparer-account activity.
- Mailbox forwarding rules, MFA prompts, unusual logins, password resets or messages not sent by the user.
- Security tools disabled, files encrypted, unexplained exports, remote-control software or missing devices.

Offline contact sheet location: [Enter secure offline location]. Last verified: [date]. Owner: [name].

Use counsel and current source guidance; timing can run from discovery, not final certainty.

RECIPIENT	TRIGGER / PURPOSE	TIMING	OWNER / CONTACT	EVIDENCE
IRS Stakeholder Liaison	Suspected tax-practice client data theft	Immediately		
Cyber / professional insurer	Event or circumstance meeting policy notice terms	Per policy; promptly		
FTC	Qualifying notification event involving unencrypted customer information of at least 500 consumers	As soon as possible; no later than 30 days after discovery		
State regulators / attorneys general	State breach, tax, privacy or professional-duty trigger	Per applicable law		
Law enforcement / FBI IC3	Crime, extortion, fraud or threat requiring assistance	Promptly as advised		
Affected clients / other parties	Notice or protective action required by law, contract or risk	As directed		

Information to prepare

Collect only through an approved secure channel and follow current instructions.

- Practice contact information, PTIN / EFIN details, discovery and incident dates and a concise factual narrative.
- Affected systems, known safeguards, MFA status, preparer identifiers and a secure list of affected taxpayer identifiers if requested.
- Actions already taken, technical contacts, insurer / counsel contacts and preserved evidence locations.

Do not improvise sensitive submissions

Verify the current recipient and secure transmission method. Do not send names, addresses, Social Security numbers or other sensitive details by ordinary email unless an authorized process specifically requires it.

Recover essential services while limiting unnecessary copies of customer information.

Continuity priorities

Define measurable recovery objectives and safe fallback methods.

CRITICAL SERVICE	OWNER	RECOVERY TARGET	DEPENDENCIES / FALLBACK	LAST TEST / RESULT
Client communication				
Tax preparation and e-file				
Portal and document access				
Payroll / bookkeeping				
Identity, email and administration				

Retention and disposal schedule

Tie each category to a legitimate requirement and verifiable destruction method.

RECORD / MEDIA	RETENTION BASIS / PERIOD	SYSTEM OWNER	DISPOSAL METHOD	EVIDENCE
Client tax and identity records				
Email, portal and collaboration data				
Backups, exports and temporary files				
Devices, paper and removable media				

Legal hold: Suspend ordinary disposal when [role] issues a hold. Document scope, custodians, start date and release approval.

Turn testing and incident lessons into leadership decisions.

Qualified Individual report

Summarize the program's status and material issues for the governing body or senior officer.

REPORT ELEMENT	SUMMARY / EVIDENCE	DECISION / ACTION
Overall program status and scope		
Risk assessment and material residual risks		
Safeguard testing and monitoring results		
Service-provider arrangements		
Security events and response lessons		
Recommended changes, resources and priorities		

Change log

Update after material operational, technology, threat, incident or legal change.

VERSION	DATE	CHANGE / REASON	OWNER	APPROVAL
Report period				
Submitted by / date				
Reviewed and approved by				
Next review				

A project sequence, not a legal grace period or universal deadline.

Do not delay an existing obligation

This schedule is a practical way to organize work. It does not postpone requirements that already apply or replace faster action for a known high risk, active incident, insurer deadline or legal notice duty.

WHEN	PRIORITY ACTION	OWNER	DUE	EVIDENCE / STATUS
Days 1–3	Appoint the Qualified Individual; approve scope, contacts and document control.			
Days 1–7	Inventory information, systems, devices, integrations and service providers.			
Days 4–10	Complete the written risk assessment; escalate high risks immediately.			
Days 5–15	Confirm MFA, encryption, patching, endpoint protection and backup controls.			
Days 10–20	Review high-risk vendors, access lists, retention and remote-work controls.			
Days 12–24	Train personnel; obtain acknowledgments; verify reporting contacts offline.			
Days 18–27	Test restoration and conduct an incident tabletop exercise.			
Days 25–30	Obtain qualified review, approve the plan and schedule recurring reviews.			

Readiness gate

Before calling the plan operational, confirm that:

- ☐ Every critical safeguard has an accountable owner and evidence source.
- ☐ High risks have a dated action, approved treatment or documented escalation.
- ☐ Personnel know the immediate incident-reporting channel.
- ☐ IRS, insurer, counsel and technical contacts are current and available offline.
- ☐ Leadership approved the plan and the next review is scheduled.

Use shared language so owners, personnel and providers make consistent decisions.

TERM	PLAIN-LANGUAGE MEANING
Customer information	Nonpublic personal information about a customer handled in connection with providing a financial product or service; confirm the legal definition for this practice.
Qualified Individual	The person designated to oversee, implement and enforce the information-security program. The role may be internal or provided by an affiliate or service provider.
Safeguard	An administrative, technical or physical control used to reduce information-security risk.
Residual risk	Risk that remains after current safeguards are considered.
Service provider	A party that receives, maintains, processes or can access customer information through services to the practice.
Security event	An occurrence involving possible unauthorized access, use, disclosure, alteration, loss or destruction of information or systems.
Notification event	A defined event that may trigger notice to the FTC under the Safeguards Rule; obtain current legal review of the facts and definition.
RTO / RPO	Recovery time objective: target time to restore. Recovery point objective: acceptable amount of data loss measured in time.
MFA	Authentication requiring two or more independent factors, such as a password plus a hardware key or authenticator.
Evidence	A dated record showing a safeguard or decision exists and operates, such as settings, logs, reports, approvals or test results.

Practice-specific terms

Add terms that personnel or vendors could interpret differently.

TERM	APPROVED DEFINITION / OWNER

Verify current primary-source guidance whenever the plan is reviewed.

Primary sources

Use these sources with qualified advice when tailoring the plan.

FTC — Safeguards Rule: What Your Business Needs to Know

<https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know>

IRS Publication 5708 — Creating a WISP for Your Tax & Accounting Practice

<https://www.irs.gov/pub/irs-pdf/p5708.pdf>

IRS Publication 4557 — Safeguarding Taxpayer Data

<https://www.irs.gov/pub/irs-pdf/p4557.pdf>

IRS — Stakeholder Liaison Contacts

<https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-contacts>

FTC — Data Breach Response: A Guide for Business

<https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>

IRS — Identity Theft Information for Tax Professionals

<https://www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals>

Educational use only

This independent template is general educational information and a starting point for discussion. It is not an official IRS form; does not constitute legal, cybersecurity, tax, accounting or insurance advice; and does not guarantee compliance, security, coverage or claim payment. Requirements vary by facts and jurisdiction and can change. Consult qualified legal, cybersecurity and insurance professionals before adoption or reliance.

smallbusinessinsured.com

© 2026 Small Business Insured. Customize for your own practice; redistribution or resale requires permission.