



An Extended Guide · No. 2071

# The Written Security Plan Tax Preparers Must Have

---

What the IRS expects, the sample  
template, and keeping it current

**Tech Made Simple — Service Made Personal**

[BillsHomeTech.com](http://BillsHomeTech.com) · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —  
[billshometech.com/book](http://billshometech.com/book)

**! Read this first — the two things that stop most attacks**

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. For a tax preparer those habits aren't just smart — a written data security plan built around them is something the IRS expects every professional preparer to have.

**The written plan every tax preparer is expected to have**

If you prepare tax returns for pay, the IRS expects you to keep a written data security plan — often called a WISP, a Written Information Security Plan. It's not optional, and it ties to your PTIN. This guide explains what that means in plain English, and how to get one done without stress.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping small businesses get comfortable with their technology. I'm a tech helper, not a lawyer or an enrolled agent — so think of me as the person who helps you understand the requirement, set up the safeguards, and line up the right professional for the rest.

Here's the reassuring part up front: the IRS doesn't expect a corporate security department. It expects a sensible, written plan that fits a practice your size — and it even gives you a sample template to start from. We'll walk through what's expected and how the pieces fit.

**★ I'll help you build the safeguards behind the plan**

The plan names safeguards like MFA, encryption, and backups — and those are exactly what I set up and test for small offices. I'll help you make the plan true, then you confirm the legal wording with your own advisor. Call or text me at (330) 200-8042.

## First, the honest disclaimer

Before we go further, let me be clear about what this guide is — and what it isn't.

I want you to walk away understanding the requirement well enough to act on it and to ask your tax-industry advisor the right questions. But the rules here come from federal law and IRS guidance that can change, and the exact wording on forms and publications updates from year to year.

### **! A quick, important note**

This guide explains the tax-preparer security-plan requirement in plain English so you know what to ask about — it is general information, not legal or tax advice, and it is not a substitute for the actual IRS publications and the law. Publication numbers, form lines, and requirements change, so always use the current-year IRS forms and publications and confirm the details with the IRS, a tax professional, or an attorney before you rely on anything here.

### **✓ Always use the current year's forms and pubs**

Whenever this guide names a form line or a publication, treat it as a starting point and check the current-year version at IRS.gov. The IRS updates these regularly, and your plan should reflect what's required this season, not a past one.

## The whole guide, on one page

If you remember only these things, you'll meet the requirement the right way.

- ❑ Every professional tax preparer (PTIN holder) is expected to keep a **written data security plan — a WISP**.
- ❑ The requirement flows from **federal law (GLBA) and the FTC Safeguards Rule** — see our FTC Safeguards guide.
- ❑ **IRS Publication 4557** explains what taxpayer data you must protect and your responsibilities.
- ❑ **IRS Publication 5708** is a **sample WISP template** you customize — not a fill-in-and-forget form.
- ❑ On **Form W-12** (PTIN renewal), there's a **data-security certification checkbox** — you confirm, under penalty of perjury, that you maintain a WISP.
- ❑ Name responsible people, inventory data and systems, list safeguards, train staff, plan for incidents — and review it **at least annually**.

### ! The certification is under penalty of perjury

When you renew your PTIN and check the data-security box, you're certifying under penalty of perjury that you maintain a plan consistent with your legal obligations. That's a real statement — make sure your plan actually exists and is current before you check it.

## Why tax preparers have this duty

It helps to know where the requirement comes from, because it's not an IRS whim — it's federal law.

Tax preparers handle some of the most sensitive data there is: Social Security numbers, income, bank details, dependents' information — a complete identity-theft kit for every client. Crooks know it, and tax practices are a repeated target.

Because preparers are paid to handle financial information, federal law treats them as 'financial institutions' under the Gramm-Leach-Bliley Act (GLBA) and its FTC Safeguards Rule. That law requires a written information security program. The IRS, through the Security Summit it runs with the tax industry and states, turned that obligation into plain guidance aimed at preparers — and tied it to your PTIN.

### ✓ This connects to our [FTC Safeguards guide](#)

The same FTC Safeguards Rule that requires your WISP applies to lots of other small businesses too — accountants, lenders, and more. If you want the broader picture behind the rule, our [FTC Safeguards guide](#) covers who else it catches and what it requires.

## The two IRS publications to know

The IRS hands you two documents that make this far less intimidating. Know what each one is for.

### IRS Publication 4557 — Safeguarding Taxpayer Data

This is the 'what and why.' Publication 4557 explains what taxpayer data you're responsible for protecting, the kinds of safeguards expected, and your duties as a preparer. Read it as the plain-English background to the whole requirement.

### IRS Publication 5708 — the sample WISP template

This is the 'how.' Publication 5708 is a sample Written Information Security Plan, created with the Security Summit specifically for tax and accounting practices. It gives you a structure to follow and fill in. The key word is **sample** — you must customize it to your actual practice, not just sign a blank template.

#### **! A template is a start, not a finish**

Publication 5708 is scaffolding, not a shortcut. A WISP that still describes a generic practice — not your real staff, systems, and safeguards — isn't really your plan. Fill in every blank with the truth about how you actually operate.

## The PTIN renewal checkbox

The requirement isn't just theory — it shows up every year when you renew your PTIN.

Since the 2024 PTIN cycle, Form W-12 — the form you use to apply for or renew your preparer tax ID number — includes a data-security certification checkbox, around Line 11. By checking it, you confirm, under penalty of perjury, that you are aware of your data-security responsibilities and maintain a written security plan consistent with your legal obligations.

So the practical trigger is renewal season. Before you check that box, your WISP should genuinely exist and be current — because you're making a sworn statement, not ticking a formality. Confirm the exact line number and wording on the current-year W-12, since the IRS can renumber or reword it.

### ✓ Make your WISP review part of PTIN renewal

Pin your annual WISP review to the same time you renew your PTIN. Then the checkbox isn't a moment of doubt — it's the natural end of a review you just finished, and your certification is honest by design.

## What a WISP actually contains

Strip away the jargon and a WISP is a sensible description of how you protect client data. These are the parts.

- **Responsible people:** who owns security in your practice, and who backs them up.
- **Data and systems inventory:** what client data you hold, where it lives, and what devices and services touch it.
- **Safeguards:** the administrative, technical, and physical protections you use — access controls, MFA, encryption, backups, locked files.
- **Employee training:** how your people learn to spot phishing and handle data safely.
- **Incident response:** what you'll do, and who you'll notify, if there's a breach.
- **Review:** a commitment to update the plan at least annually and when things change.

### ✓ It's the same bones as our one-page plan

If that list looks familiar, it should — it's our one-page security plan with more detail. If you've already written that one page, you're well ahead on your WISP. Our one-page security plan guide is a gentle place to start.

## The safeguards behind the plan

A WISP is only as good as the real protections it describes. These are the ones that matter most for a tax practice.

The plan names safeguards; your job is to actually have them. The good news is that the most important ones are the same basics every small business needs, and they're squarely in the realm of what I help set up and test:

- ❑ **MFA everywhere** — on email, your tax software, remote access, and any cloud storage. See our Microsoft 365 and Google Workspace sign-in guides.
- ❑ **Encryption** — disk encryption on laptops (BitLocker or FileVault) so a lost device doesn't leak client data.
- ❑ **Tested backups** — kept where ransomware can't reach, and actually restored at least once.
- ❑ **Updates current** — no end-of-support software holding client data.
- ❑ **Access control** — individual logins, least access, and no shared accounts.

### ★ These are exactly what I set up and test

MFA, disk encryption, a real backup you've restored — this is my day-to-day work for small offices. I'll make the safeguards in your WISP true and provable, so your plan isn't just paper. Call (330) 200-8042.

## Right-sizing the plan to your practice

A one-person seasonal preparer and a ten-person firm both need a WISP — but not the same WISP.

The requirement scales to the size and complexity of your practice. A solo preparer working from a home office writes a shorter, simpler plan than a firm with staff, multiple locations, and a network. Neither is wrong; each should honestly reflect how that practice actually operates.

So don't copy a large firm's elaborate plan if you're a one-person shop — it'll describe a practice you don't run, which defeats the purpose. Start from the IRS sample template and keep only what's true for you, written plainly. A short honest plan beats a long borrowed one.

### ✓ Honest and yours beats long and borrowed

An underwriter, an IRS reviewer, or a client who asks will see through a generic plan immediately. The plan that protects you is the one that describes your real staff, your real systems, and your real safeguards — however short that makes it.

## The same duty, a different-sized plan

Every PTIN holder needs a WISP, but what yours looks like depends on whether you're a solo seasonal preparer or a firm with staff.

### If you're a solo or seasonal preparer

Working alone, often from home and heaviest in season, your plan is short and personal — but it still has to exist, be customized, and be current when you certify on your PTIN renewal.

- Your 'responsible person' is you; name a trusted backup who could reach your systems in an emergency.
- Keep the data inventory simple — your tax software, email, and where client files are stored.
- Nail the personal safeguards: MFA, an encrypted laptop, a tested backup, a locked file cabinet.
- Review and date the plan each year before you renew your PTIN and check the box.

### If you run a firm with staff

With employees handling client data, your WISP has to cover people and process — who has access to what, how they're trained, and what happens when someone joins or leaves.

- Name a clear security lead and spell out who may access which client data.
- Document employee training on phishing and safe data handling — and keep a record you did it.
- Cover onboarding and offboarding so access is granted and cut cleanly — see our offboarding guide.
- Address any vendors or cloud services that touch client data, and your incident-response steps.

#### ★ Not sure how big your plan needs to be?

Tell me how your practice runs — solo or staffed, home or office, what software you use — and I'll help you build safeguards that fit and a plan that honestly describes them. Call (330) 200-8042.

## Keeping the plan current

A WISP isn't a one-time chore. The requirement includes keeping it alive — reviewed at least annually and when things change.

Your plan should be reviewed and updated at least once a year, and any time your practice changes in a meaningful way: new staff, new tax software, a move to the cloud, a new office, or a security incident. Each of those can change what you protect and how, so the plan has to keep up.

Date every review. A plan marked 'last reviewed' with a recent date shows it's a living document — which is exactly what the certification, an IRS reviewer, or your insurer wants to see. An undated plan from years ago looks like what it is: forgotten.

### ✓ One calendar reminder does most of the work

Set a single annual reminder tied to PTIN renewal: review the plan, confirm the safeguards are still on, update anything that changed, re-date it, then certify. That one habit keeps you honest and current year after year.

## Building your WISP, step by step

Here's a calm path from nothing to a finished, honest plan.

- ❑ Download the current-year IRS Publication 5708 (the sample WISP) and Publication 4557 from IRS.gov.
- ❑ Inventory your client data and the systems and devices that touch it.
- ❑ Check which safeguards you already have — MFA, encryption, backups — and note the honest gaps.
- ❑ Fill in the template with your real practice: people, systems, safeguards, training, incident steps.
- ❑ Close the biggest safeguard gaps (MFA, encryption, a tested backup).
- ❑ Date it, store it safely, and set an annual review tied to PTIN renewal.

### ★ Let's do the technical half together

You own the plan and the legal wording; I can handle the technical safeguards — turning on MFA, encrypting the laptops, testing a real backup — so the plan you write is actually true. Call (330) 200-8042.

## What the WISP is — and isn't

A few quick clarifications save a lot of confusion about what this requirement actually asks of you.

A WISP is a written plan you keep and maintain — not something you file with the IRS or get approved or certified by anyone. Nobody stamps it. You keep it, you follow it, you certify on your PTIN renewal that it exists, and you produce it if you're ever asked (for example, after an incident or in an inquiry).

It's also not a one-time purchase or a signed form that makes you 'compliant' forever. There's no magic document or product that handles this for you. The requirement is ongoing: a real plan, real safeguards, and a yearly review. Be wary of anyone selling instant, permanent compliance.

### **! No product makes you 'instantly compliant'**

You'll see software and services promising to make you Safeguards- or WISP-compliant in a click. Tools can help you meet the requirement, but none of them replace having a real, customized plan and actually following it. If a pitch sounds too easy, be skeptical.

## If client data is ever exposed

Your WISP should include incident-response steps — here's the plain-English shape of what to do.

If you suspect a breach of client data, your plan should already name who to call and in what order. Stay calm, isolate the affected system, and work your call list. For tax preparers there's an extra wrinkle: the IRS and the tax-industry Security Summit have specific guidance on reporting data theft, so confirm the current steps and who to notify.

- **Follow your WISP's incident steps** — that's what they're for.
- **Call your insurer's hotline** if you carry cyber coverage — they direct the response. See our cyber-insurance guides.
- **Report per current IRS guidance** for tax-professional data theft — confirm who to contact this year.
- **Report to the FBI's IC3 ([ic3.gov](https://ic3.gov))** for the internet-crime side.
- **Check Ohio breach-notification duties** — see our Ohio breach guide; a lawyer confirms who must be told.

### ✓ Know the reporting steps before you need them

The middle of a breach is the worst time to figure out who to call. Write the current tax-professional reporting contacts into your WISP now, and confirm them at your annual review, so the answer is already on the page.

## Your tax software and vendors count too

Protecting client data isn't only about your own office — it includes the services you trust with that data.

Your tax-prep software, cloud storage, document portals, and any outside IT help all touch client information, so your plan should account for them. Turn on every security feature your tax software offers — especially MFA — and understand how it stores and protects data.

If you use outside IT help, keep control of the things that matter: your admin accounts, your domain, and a list of who can reach your systems. Never hand over the only copy of the keys. Our guide on hiring outside IT help covers what to keep in your own hands.

### ✓ MFA on your tax software is non-negotiable

The login to your tax-prep software guards a season's worth of client identities. If it offers multi-factor authentication — and reputable ones do — turn it on for every user, no exceptions. It's one of the highest-value safeguards in your whole plan.

## Training the people who touch client data

Your plan assumes your staff can spot a scam and handle data safely. A little training makes that true.

Most breaches start with a convincing email, not a clever hack, so the people in your practice are both your biggest risk and your best defense. Your WISP should note that staff are trained, and you should keep a simple record that it happened — a date and who attended is enough.

Keep the training practical and short. Show real-looking phishing examples, cover the fake-invoice and 'new bank details' scam (see our call-back-rule guide), and make clear that it's always okay to slow down and verify. Refresh it before each busy season, when attackers ramp up.

### ✓ Write down that you trained — and when

A one-line note — 'phishing and data-handling training, with dates and attendees' — turns a vague 'we talk about it' into something your plan can point to. It's easy to do and exactly the kind of evidence that shows the plan is real.

## The mistakes that undercut a WISP

Nearly every weak plan I see falls into one of these traps. Now you'll steer clear.

- **Checking the W-12 box without a real plan** — that's a sworn statement; make sure the plan exists first.
- **Signing the template unchanged** — a generic, uncustimized WISP isn't really your plan.
- **Describing safeguards you don't have** — write the truth, then close the gaps.
- **Never reviewing it** — a stale plan describes a practice you no longer run.
- **Skipping MFA on your tax software or email** — the highest-value safeguard, often missed.
- **Relying on an old publication** — always use the current-year IRS forms and pubs.

### **! A paper plan with no real safeguards helps no one**

The worst outcome is a tidy WISP sitting in a drawer while MFA is off and backups are untested. The document is not the point — the protection is. Make the plan describe safeguards that genuinely exist, then keep them running.

## Get it done this season

If you don't yet have a WISP, here's the short path to a real one before your next renewal.

- ❑ Pull the current IRS Pub 5708 (sample WISP) and Pub 4557 from IRS.gov.
- ❑ List your client data, your systems, and your devices.
- ❑ Turn on the big safeguards: MFA on email and tax software, an encrypted laptop, a tested backup.
- ❑ Customize the template with your real practice and honest safeguards.
- ❑ Train your people and jot the date and attendees.
- ❑ Date the plan, store it safely, set an annual review tied to PTIN renewal — then certify honestly.

### ★ I'll handle the tech so you can finish the plan

Give me the technical to-dos — MFA, encryption, a real backup, locking things down — and I'll make them true and show you the proof. You write the plan around safeguards that actually work. Call (330) 200-8042.

## Keep proof your plan is real

A WISP is stronger when you can show the safeguards it names are genuinely in place.

For each safeguard your plan describes, keep simple, dated evidence: a screenshot of MFA turned on for your tax software and email, a note of the date you tested a backup restore, a record that your laptops are encrypted, the date and attendees of staff training. Store it with the plan itself.

This little evidence file does double duty. It backs up your penalty-of-perjury certification, and if you ever carry cyber insurance, it's the same proof our cyber-insurance application guide tells you to keep. One tidy folder serves both purposes.

### ✓ A one-page evidence sheet ties it together

List each safeguard in your WISP and, next to it, where the proof lives and the date you last confirmed it. That single sheet turns a nervous audit or claim into a calm five-minute task.

## How this fits the bigger picture

Your WISP doesn't stand alone — it's one corner of staying safe and compliant, and it links to several sibling guides.

- The **FTC Safeguards Rule** is the law behind your WISP — our FTC Safeguards guide covers who else it catches.
- The **one-page security plan** guide is the gentle starting point for the same bones.
- The **Microsoft 365 and Google Workspace** guides show how to turn on the MFA your plan requires.
- The **backup fire-drill** guide turns 'we have backups' into 'we've tested them.'
- The **cyber-insurance** guides explain coverage that pairs with — but doesn't replace — your safeguards.

### ✓ Build the habit once, use it everywhere

The work you do for your WISP — MFA, encryption, tested backups, trained staff — is the same work that protects you generally, lowers your insurance cost, and answers a client's security questions. Do it once; it pays off in every direction.

## Common Questions

The questions I hear most from preparers facing the WISP requirement, answered plainly.

### **Q: Do I really need a WISP if I'm a solo, seasonal preparer?**

Yes. The requirement applies to professional tax preparers generally, not just firms — it flows from federal law (GLBA and the FTC Safeguards Rule). Your plan can be short and simple, scaled to a solo practice, but it still needs to exist, be customized, and be current.

### **Q: Where do I get a template, and is it enough to just sign it?**

The IRS offers a sample WISP in Publication 5708, created with the Security Summit. It's a great start — but you must customize it to your real practice. Signing the generic template unchanged isn't truly your plan. Use the current-year version from IRS.gov.

### **Q: What's the checkbox on the PTIN renewal about?**

Since the 2024 cycle, Form W-12 includes a data-security certification checkbox, around Line 11. Checking it confirms, under penalty of perjury, that you maintain a written security plan consistent with your obligations. Make sure your WISP is real and current before you check it, and confirm the current line and wording.

### **Q: Do I file my WISP with the IRS?**

No. You keep and maintain it — nobody approves or certifies it. You certify on your PTIN renewal that it exists, follow it, review it at least annually, and produce it if you're ever asked. There's no magic product that makes you permanently compliant.

### **Q: What's the single most important safeguard to get right?**

Multi-factor authentication on your email and your tax software. Those logins guard a season's worth of client identities, and turning on MFA is the highest-value, lowest-cost thing you can do. Our sign-in guides show you how.

#### **★ Facing the WISP requirement right now?**

Give me a call and we'll sort the technical safeguards together — MFA, encryption, a tested backup — so the plan you write is honest and your certification is true. I'll line you up with the right advisor for the legal wording. Call or text (330) 200-8042.

## You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made your tax-preparer security plan feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't worry about memorizing anything.

When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I'm a tech helper, not a lawyer or your insurance agent — for the legal and insurance pieces I'll help you understand the questions and line up the right professional.

### ★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

## The Two IRS Publications

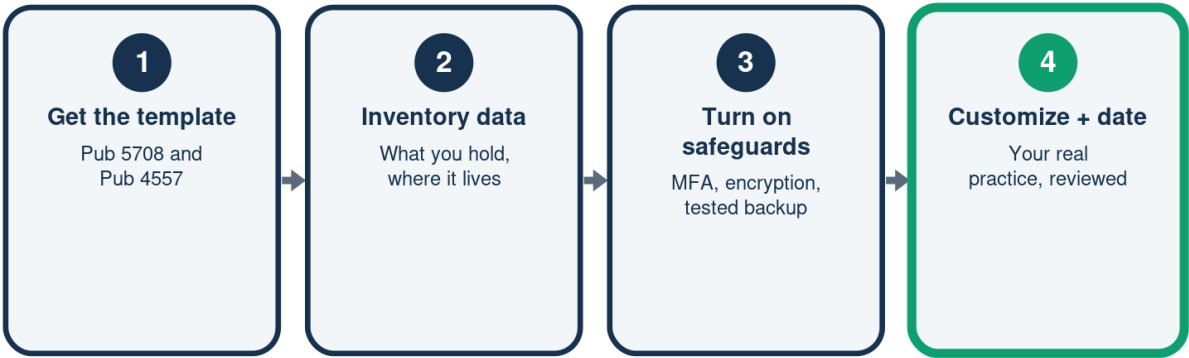
What each one is for

|              | What it is       | Your job         |
|--------------|------------------|------------------|
| Pub 4557     | The what and why | Read it          |
| Pub 5708     | Sample WISP      | Customize it     |
| Form W-12    | Cert checkbox    | Certify honestly |
| Current year | Use the latest   | Check IRS.gov    |

Always use the current-year versions from IRS.gov.

## Build Your WISP in Four Steps

From sample template to an honest plan



Review at least yearly, tied to PTIN renewal, before you certify.

## What Goes In a WISP

The sensible parts of the plan

| In plain terms |                   | You write       |
|----------------|-------------------|-----------------|
| People         | Who's responsible | Names + backup  |
| Inventory      | Data and systems  | Where it lives  |
| Safeguards     | MFA, encryption   | Backups, access |
| Incident plan  | Who to call       | The steps       |

Same bones as our one-page plan, with more detail.





## Need a Real Person?

You do not have to remember all of it.  
You just have to remember you can call.  
Friendly, in-person tech help -- I come to you.

### BILL'S PROMISE

If you are not 100% happy with a visit, I will  
make it right -- or refund it. No awkwardness,  
no fine print. That is how I would want to be treated.

**(330) 200-8042 · BillsHomeTech.com**

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

---

### Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



## A Note From Bill

### A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —  
[billshometech.com/book](https://billshometech.com/book)

Use of these guides is subject to our Terms of Use ([billshometech.com/terms-of-use](https://billshometech.com/terms-of-use)).

**(330) 200-8042 · BillsHomeTech.com**

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech