

Is Your Tax Practice WISP-Compliant?

A 10-Point Self-Check for CPAs, EAs & Tax Preparers

If you prepare returns for compensation, a WISP is not optional. The Gramm-Leach-Bliley Act and the **FTC Safeguards Rule (16 CFR Part 314)** treat tax and accounting practices as financial institutions, and **IRS Publications 4557 and 5708** spell out what your **Written Information Security Plan (WISP)** has to contain. There is no revenue threshold, no headcount minimum, and no carve-out for solo practitioners — and at PTIN renewal, **Form W-12, Line 11** asks you to acknowledge the requirement in writing.

How to use this: Go down the list and honestly check every box you can answer "yes, and we could show it" to. Your total points you to where the gaps are — and what to fix first, before filing season starts.

The 10-Point Check ◇◇◇

- 1 ☐ **You have an actual written WISP document**
A real document — written down, dated, and reviewed within the last 12 months. Not verbal policy, not good habits, and not a template someone downloaded and never finished. It is the first thing anyone asks for.
- 2 ☐ **One named person owns the program**
The Safeguards Rule requires a designated **Qualified Individual** — an owner, office manager, or your IT provider — who is accountable for maintaining the plan and its safeguards.
- 3 ☐ **You've done a written risk assessment**
A documented assessment of the foreseeable threats to client data, in writing and revisited periodically. A mental inventory of what worries you does not satisfy the rule.
- 4 ☐ **You know exactly where client data lives**
Every place a return, K-1, Social Security number, or bank detail sits: your tax software, email, the client portal, cloud storage, backups, paper files, and every laptop that leaves the office in March.
- 5 ☐ **Access is limited, with MFA on everything**
Only staff who need client data can reach it, with unique logins and multi-factor authentication across tax software, email, remote access, and the portal — not just the systems that forced you into it. No shared passwords.

The 10-Point Check (continued)

6 ☐ Client data is encrypted at rest

Returns and client PII are encrypted on servers, workstations, laptops, portable drives, and backups — so a device lost during filing season isn't a reportable breach.

7 ☐ Client data is encrypted when it travels

Documents move through a secure client portal, not as plain email attachments. Anything sent over the internet or wirelessly — to clients, to staff, to the IRS — is transmitted securely.

8 ☐ Systems are patched and protected

The IRS "Security Six" — anti-virus, firewall, multi-factor authentication, backup, drive encryption, and a VPN for remote access — running, current, and on every system connected to the internet.

9 ☐ Your vendors are vetted and under contract

Every third party that touches client data — tax software host, cloud provider, IT provider, document shredding — is selected for adequate safeguards and contractually required to protect it.

10 ☐ Staff are trained, with an incident plan ready

Your team is trained on phishing, refund fraud, and wire fraud, with records to show it — and you have a written incident-response and breach-notification plan, including who to contact at the IRS, before you need it.

What your score means



9–10

Strong footing. You likely have the bones of a compliant program. Make sure it's written down, dated, and reviewed — an undated WISP still fails under scrutiny.

5–8

Real gaps. You have pieces in place, but the missing controls are exactly what an IRS inquiry, an FTC examiner, or a cyber-insurance application will surface. Close them before January.

0–4

Significant exposure. You most likely don't have a compliant WISP — a federal obligation today, and a breach without one is far harder to defend.

Why it matters for tax practices



Federal, not optional

The GLBA and FTC Safeguards Rule cover tax and accounting practices as financial institutions. IRS Pub 4557 and Pub 5708 define what's expected. Practice size does not exempt you.

Tied to your PTIN

Form W-12, Line 11 asks you to acknowledge that paid preparers are required by law to create and maintain a WISP. Renewal runs from mid-to-late October through December 31.

Season-ending risk

Ransomware in March costs you the season. Carriers also now require MFA, monitoring, and tested backups before they'll write a cyber policy — the same controls listed above.

FREE • NO OBLIGATION

Not sure how your practice scored?

If any of these points were hard to answer — or you'd like help building, updating, or reviewing your firm's WISP — we're glad to help. Ask IT Support RI for a complimentary **Tax Practice Security & WISP Readiness Review** and we'll walk through every point with you. No pressure, no obligation.

Talk to us → ITsupportRI.com/contact-us

Main: 401-522-5200 • MA: 508-618-5774 • Web: ITsupportRI.com