Work through one section per week and you'll have materially hardened your practice inside two months. Items marked **(WISP)** map to elements commonly required in a Written Information Security Plan under the FTC Safeguards Rule — tax preparers are required to maintain one.

Ready to formalize it? Once you've worked the checklist, turn it into the document the IRS expects with our free, editable Written Information Security Plan (WISP) template.

Identity & access

- [ ] Multi-factor authentication enforced on email, tax software, cloud storage, and banking — no exceptions **(WISP)**
- [ ] A password manager deployed firm-wide; no shared spreadsheets of passwords
- [ ] Unique credentials per person — no shared logins, even for admin staff
- [ ] Off-boarding checklist that revokes every account the same day someone leaves **(WISP)**
- [ ] Quarterly review of who has access to what; least-privilege by default **(WISP)**
- [ ] Separate admin accounts from daily-driver accounts

Devices

- [ ] Full-disk encryption on every laptop and desktop (BitLocker / FileVault) **(WISP)**
- [ ] Automatic OS and browser updates enabled everywhere
- [ ] Endpoint protection installed and reporting centrally
- [ ] Screen-lock timeout of 10 minutes or less
- [ ] Firm data blocked or containerized on personal phones; mobile PIN + biometrics required
- [ ] Old machines wiped (not just deleted) before disposal — keep a disposal log **(WISP)**

Data

- [ ] Client data inventory: know where every SSN and EIN lives **(WISP)**
- [ ] Backups: automatic, tested by restoring a file quarterly, one copy off-site/ immutable **(WISP)**
- [ ] Retention policy applied — old client files archived or destroyed on schedule **(WISP)**
- [ ] Portal or encrypted email for every document exchange; no tax documents over plain email

- [ ] Cloud storage sharing links default to “specific people,” never “anyone with link”
- [ ] Spreadsheet exports containing client data password-protected or avoided

Email & phishing

- [ ] SPF, DKIM, and DMARC records published for your domain
- [ ] External-sender banner on inbound mail
- [ ] Wire/payment-change requests verified by phone at a known number, every time
- [ ] Annual phishing awareness exercise — even a small informal one **(WISP)**
- [ ] Suspicious-message reporting path everyone actually knows

Vendors & software

- [ ] Vendor list with data-access notes reviewed annually **(WISP)**
- [ ] Tax software, portal, and hosting providers’ security pages reviewed
- [ ] Unused software and browser extensions removed
- [ ] AI tools governed by policy (see our AI Use Policy Template)

Incident response

- [ ] One-page incident plan: who to call, in what order, including cyber insurer and the IRS Stakeholder Liaison for data theft **(WISP)**
- [ ] Cyber liability insurance in force; policy requirements (MFA, backups) actually met
- [ ] Contact sheet printed — useful when systems are down
- [ ] A data-incident tabletop conversation held once a year **(WISP)**
- [ ] Designated security coordinator named in your WISP **(WISP)**

The two-hour quick start

If you do nothing else this month: enforce MFA everywhere (45 min), deploy a password manager (30 min), verify backups restore (30 min), and publish the incident contact sheet (15 min). Those four items eliminate the majority of real-world small-firm incidents.
