THINK OUTSIDE THE TAX BOX

THE PREMIER TAX REDUCTION SOURCE

CYBER SECURITY CHECKUP

Governance & Compliance

- I have a Written Information Security Plan (WISP).
- My WISP includes: risk assessment, access controls, encryption policy, incident response plan, vendor management, employee training.
- I have designated a Qualified Individual (QI).
- I attest truthfully during PTIN renewal that I have a WISP.
- I have a GLBA-compliant Privacy Policy.
- I understand IRC §7216 restrictions.
- If I serve California clients, I know Cal. Civ. Code §1798.82 breach rules.

Access Controls & Authentication

- MFA is enabled on: email, tax software, portals, cloud storage.
- I use a password manager.
- No shared logins; all staff have unique accounts.
- All passwords are long and random.
- MFA emergency codes stored securely.

Secure Communication

- All taxpayer documents go through portal — never email.
- I have a written communication policy for clients.
- Email is encrypted.
- I warn clients regularly about IRS phishing scams.

Device, Network & Physical Security

- OS updates applied weekly; software auto-updates on.
- Business-grade firewall/router installed.
- Office Wi-Fi uses WPA3 and strong password.
- Guest network used for visitors and personal devices.
- All drives encrypted.
- Screens auto-lock after 5–10 minutes.
- Remote wipe enabled on devices.

Data Storage, Backup & Retention

- All taxpayer data is stored encrypted.
- I follow the 3-2-1 backup rule.
- Backups are tested quarterly.
- Old files are purged per retention policy.
- No unencrypted USB drive storage.

Vendor Management

- I review vendor security annually.
- Vendors handling client data sign data-protection agreements.
- I confirm vendors use MFA, encryption, and provide breach notifications.
- I do not rely solely on my IT provider.

AI Usage

- I never enter PII into AI tools.
- My WISP includes an AI usage policy.
- Staff are trained on AI safety rules.

Client Management & Training

- Clients receive onboarding instructions for secure document exchange.
- The portal is required for sending PII.
- Policies are reinforced at least annually.
- The engagement letter includes cybersecurity expectations.

Employee Training & Human Risk

- Annual cybersecurity awareness training is completed.
- Staff know how to spot phishing, vishing, and smishing.
- Staff understand password, device, and incident policies.
- Staff know never to email PII.

Incident Response & Breach Procedures

- I know who to contact: IRS Stakeholder Liaison, state agency, software vendor, insurer.
- I have a written breach response plan.
- I maintain logs of access and activity.
- I rehearse or review incident response steps regularly.

Cyber Insurance

- My policy covers breach response, legal fees, ransomware, and business interruption.
- My insurer requires MFA, a WISP, and backups — and I comply.

Annual Review Checklist

- My WISP is reviewed and updated.
- Passwords and user accounts are audited.
- Backups are tested.
- Vendors are evaluated.
- Insurance coverage is reviewed.
- A security self-assessment is completed.
- Policies are updated as laws change.

Final 4 Actions

1

Enable MFA everywhere

2

Use a client portal - no email

3

Update systems weekly

4

Implement and maintain your WISP