FREE WISP TEMPLATE

IRS Written Information Security Plan (WISP) Template for CPA Firms

Publication 4557 compliance checklist with 38 action items.
Every tax preparer needs this — regardless of firm size.

Joe Crist
CEO & Founder, Transform 42 Inc.
Service-Disabled Veteran-Owned Small Business
Miami & South Florida

WISP Foundation & Governance

IRS Publication 4557, Section 2 — Required plan structure and responsible parties

Plan Documentation

- [ ] **Create a written WISP document** — IRS requires all tax preparers to have a written security plan. Not optional. Not verbal. Written. Pub 4557, p.2
- [ ] **Designate a Security Coordinator** by name and title (can be the firm owner for small practices). This person owns WISP compliance. FTC Safeguards Rule §314.4(a)
- [ ] **Inventory all systems storing taxpayer data**: tax software (CCH Axcess, Drake, Lacerte, UltraTax), document management, email, scanners, external drives, cloud storage
- [ ] **Identify all categories of taxpayer PII** you handle: SSNs, EINs, bank account numbers, income data, dependent information, prior year returns
- [ ] **Document your data flow** — how taxpayer data enters your firm (client portal, email, paper), where it's stored, who accesses it, and how it's disposed of

Risk Assessment

- [ ] **Conduct an annual risk assessment** identifying threats to taxpayer data: phishing, ransomware, disgruntled employees, lost devices, client portal vulnerabilities FTC Safeguards §314.4(b)
- [ ] **Assess vendor risks** for all third parties with access to taxpayer data: cloud tax software, IT provider, document storage, client portal, bank integration partners
- [ ] **Document risk ratings** (High/Medium/Low) for each identified threat with specific mitigation controls for each

IRS enforcement is real: Circular 230 §10.36 requires firm owners to ensure adequate procedures are in place. The IRS can sanction preparers who fail to protect client data. In 2025, the IRS increased Pub 4557 compliance audits targeting firms without documented WISPs.

Access Controls & Authentication

Pub 4557 — Who can access taxpayer data and how they prove identity

User Access Management

- [ ] **Unique login credentials for every user** — no shared CCH/Drake/Lacerte logins. Each staff member gets their own account with individual audit trail. Pub 4557, p.6
- [ ] **Enable MFA on everything**: tax software, email (Microsoft 365 / Google Workspace), client portal, remote access, cloud storage, bank connections. Non-negotiable. Pub 4557, p.7
- [ ] **Role-based access** — seasonal preparers get access only to their assigned clients. Admin staff can't access return data unless job requires it. Partners see all; staff sees assigned only.
- [ ] **Remove access immediately upon termination** — disable all accounts (AD/Entra ID, tax software, email, VPN, client portal) same day. Critical during post-busy-season layoffs.
- [ ] **Password policy: 14+ characters**, no password reuse across systems. Use a firm-wide password manager (1Password Business, Keeper) for shared service accounts.

Physical Access

- [ ] **Lock the server room / network closet** — badge or key access only. No propping doors open during busy season. Pub 4557, p.8
- [ ] **Clean desk policy** — no client tax returns, SSN documents, or bank statements left on desks overnight. Shred bins at every workstation.
- [ ] **Visitor policy** — clients and vendors sign in, are escorted, and never left alone near workstations with active sessions

Busy season reality check: The biggest WISP violations happen February through April. Seasonal staff with excessive access, shared logins to save time, unlocked workstations during 14-hour days. Build your controls for the worst-case scenario — tax season.

Data Protection & Encryption

Pub 4557 — Protecting taxpayer data at rest, in transit, and during disposal

Encryption Requirements

- [ ] **Encrypt all devices storing taxpayer data**: BitLocker on Windows, FileVault on Mac. Every laptop, desktop, and external drive. Pub 4557, p.9
- [ ] **Encrypted email for sending tax documents** — Microsoft Purview Message Encryption, Virtru, or secure client portal. Never send SSNs or returns via unencrypted email.
- [ ] **Secure client portal** for document exchange (SafeSend, Citrix ShareFile, Canopy, or built-in CCH/Drake portals). Disable plain email uploads. Pub 4557, p.10
- [ ] **VPN for all remote access** — preparers working from home must connect via VPN (WireGuard, FortiClient, Cisco AnyConnect). No direct RDP exposure to the internet.

Backup & Recovery

- [ ] **Daily encrypted backups** of all tax data with 3-2-1 strategy: 3 copies, 2 media types, 1 offsite. Test restores quarterly. Pub 4557, p.11
- [ ] **Immutable/air-gapped backups** to survive ransomware (Veeam immutability, Datto, AWS S3 Object Lock). If ransomware hits during tax season, you need to recover in hours, not weeks.
- [ ] **Document RPO/RTO targets**: How much data can you afford to lose (RPO < 4 hours) and how fast must you be back online (RTO < 8 hours)?

Data Disposal

- [ ] **Shred all paper documents** containing taxpayer PII using cross-cut shredder (not strip-cut). Document shredding schedule. Pub 4557, p.12
- [ ] **Securely wipe electronic media** before disposal using NIST 800-88 compliant methods. Keep certificates of destruction for decommissioned drives.
- [ ] **Data retention policy** — define how long you keep returns, workpapers, and client documents (typically 7 years for tax records). Destroy on schedule.

Monitoring, Training & Incident Response

Pub 4557 — Ongoing vigilance and breach readiness

Security Monitoring

- [ ] **Endpoint protection on all devices** — Microsoft Defender for Business, SentinelOne, or CrowdStrike. Free antivirus is insufficient for a tax practice. Pub 4557, p.13
- [ ] **DNS filtering** to block malicious domains — Cisco Umbrella, DNSFilter, or Cloudflare Gateway. Prevents phishing links from reaching staff.
- [ ] **Enable audit logging** on tax software, email, and file servers. Review monthly for anomalies: bulk data exports, off-hours access, failed login attempts.
- [ ] **Patch management** — all systems patched within 30 days of critical updates. Automate via Intune, WSUS, or your MSP's RMM tool.

Staff Training

- [ ] **Annual security awareness training** for all staff, including seasonal preparers. Cover phishing, social engineering, and safe data handling. Pub 4557, p.14
- [ ] **Quarterly phishing simulations** — test your team with realistic IRS, client, and vendor impersonation emails. Track click rates and remediate repeat offenders.
- [ ] **Document training completion** with dates, topics covered, and attendee signatures. Auditors will ask for this.

Incident Response & Breach Notification

- [ ] **Written Incident Response Plan** with named response team, escalation procedures, and contact information for IRS, FBI, and state AG. Pub 4557, p.15
- [ ] **Know your notification obligations**: Report data theft to IRS stakeholder liaison (local), FBI IC3, FTC IdentityTheft.gov, and affected state AGs within required timelines.
- [ ] **IRS Form 14039** — know the process for filing Identity Theft Affidavits on behalf of affected clients whose data was compromised.

- [ ] **Annual tabletop exercise** — walk through a ransomware-during-tax-season scenario with your team. Document the drill and findings.

IRS Data Theft Reporting: If you suspect client data was stolen, contact your IRS Stakeholder Liaison immediately. They'll flag affected SSNs to prevent fraudulent returns. Speed matters — fraudulent returns can be filed within hours of a breach.

Need a WISP Built for Your Firm?

Transform 42 builds custom Written Information Security Plans for CPA firms in Miami and South Florida. We configure the technical controls, set up encrypted client portals, deploy endpoint protection, and keep your firm IRS-compliant year-round — including through the chaos of busy season.

Book a Free IT Security Assessment

Joe Crist — CEO & Founder
joe.crist@transform42inc.com | (424) 955-6238
transform42inc.com
Service-Disabled Veteran-Owned Small Business

LinkedIn **Facebook** **Instagram**

© 2026 Transform 42 Inc. All rights reserved. This template is for informational purposes only and does not constitute legal or tax advice.
Consult a qualified tax attorney for guidance specific to your practice.