TAX PREPARER WISP SECURITY AUDIT CHECKLIST

Written Information Security Plan (WISP) Compliance Verification & Controls Audit

Firm / Practice Name:		**Audit Date:**	
Qualified Individual (QI):		**Total Systems in Scope:**	
Auditor / Reviewer:		**Next Annual Review:**	

1. Governance & Risk Management

ID	Security Control Requirement	Priority	Status	Required Evidence / Notes
WISP-01	Designate a Qualified Individual (QI) in writing responsible for overseeing, implementing, and enforcing the WISP.	High	☐ Met ☐ Not Met ☐ N/A	Signed QI Appointment Memo
WISP-02	Map all physical and digital PII data flows, intake channels, and storage locations.	High	☐ Met ☐ Not Met ☐ N/A	PII Data Flow Map & Inventory
WISP-03	Maintain an up-to-date hardware and software asset register (including firm-owned and BYOD devices).	Medium	☐ Met ☐ Not Met ☐ N/A	Asset Inventory Register
WISP-04	Conduct and document an annual written Risk Assessment evaluating internal and external threats.	High	☐ Met ☐ Not Met ☐ N/A	Annual Risk Assessment Report
WISP-05	Deliver a written annual QI status report to firm leadership covering compliance and security events.	Medium	☐ Met ☐ Not Met ☐ N/A	Annual QI Leadership Report

2. Technical Safeguards (IRS Security Six & FTC Mandates)

ID	Security Control Requirement	Priority	Status	Required Evidence / Notes
WISP-06	Enforce Multi-Factor Authentication (MFA) on all tax preparation software, email, cloud storage, and remote portals.	High	☐ Met ☐ Not Met ☐ N/A	MFA Configuration Logs
WISP-07	Enable AES-256 full-disk encryption (BitLocker / FileVault) on all workstations and laptops.	High	☐ Met ☐ Not Met ☐ N/A	Device Encryption Status Log
WISP-08	Configure active hardware/software firewalls and isolate guest Wi-Fi from internal production networks.	High	☐ Met ☐ Not Met ☐ N/A	Firewall & VLAN Config
WISP-09	Deploy auto-updating Endpoint Detection & Response (EDR) or anti-malware software on all endpoints.	High	☐ Met ☐ Not Met ☐ N/A	EDR Console Device Report
WISP-10	Enforce encrypted VPN connections for all remote and public Wi-Fi access to firm systems.	Medium	☐ Met ☐ Not Met ☐ N/A	VPN Policy & Access Logs

WISP-11	Maintain automated daily 3-2-1 backups (including an immutable offsite cloud copy) and perform quarterly test restores.	High	☐ Met ☐ Not Met ☐ N/A	Backup & Restore Test Logs
WISP-12	Enforce Role-Based Access Control (Least Privilege), unique user IDs, 12+ character passwords, and 5-minute auto-screen locks.	Medium	☐ Met ☐ Not Met ☐ N/A	Access Control & GPO Audit

3. Physical Safeguards & Media Disposal

ID	Security Control Requirement	Priority	Status	Required Evidence / Notes
WISP-13	Keep exterior office doors locked after business hours and require visitor sign-in and escort in PII areas.	Medium	☐ Met ☐ Not Met ☐ N/A	Visitor Logbook & Lock Policy
WISP-14	Store all physical tax files, source documents, checks, and backup drives in locked, fire-resistant cabinets.	High	☐ Met ☐ Not Met ☐ N/A	Physical Storage Inspection
WISP-15	Enforce a Clean Desk / Clean Screen policy and install privacy filters on monitors visible to public/reception areas.	Low	☐ Met ☐ Not Met ☐ N/A	Office Walkthrough Checklist
WISP-16	Cross-cut shred expired paper PII (DIN P-4+) and cryptographically wipe or physically destroy obsolete drives/media.	Medium	☐ Met ☐ Not Met ☐ N/A	Certificates of Destruction

4. Administrative, Personnel & Vendor Safeguards

ID	Security Control Requirement	Priority	Status	Required Evidence / Notes
WISP-17	Conduct pre-employment background checks on all new hires, seasonal preparers, and interns prior to PII access.	High	☐ Met ☐ Not Met ☐ N/A	Background Check Clearance Log
WISP-18	Conduct mandatory cybersecurity and phishing awareness training at onboarding and at least annually thereafter.	High	☐ Met ☐ Not Met ☐ N/A	Signed Training Attendance Log
WISP-19	Execute formal onboarding and same-day offboarding checklists to provision and immediately revoke system/building access.	High	☐ Met ☐ Not Met ☐ N/A	Completed Offboarding Records
WISP-20	Collect SOC 2 reports, security summaries, and written safeguards commitments from all third-party vendors handling PII.	Medium	☐ Met ☐ Not Met ☐ N/A	Vendor Due Diligence File
WISP-21	Configure multi-office badge access and server room physical access controls (if applicable to firm footprint).	Low	☐ Met ☐ Not Met ☐ N/A	Facility Access Control Log

5. Testing, Monitoring & Incident Response

ID	Security Control Requirement	Priority	Status	Required Evidence / Notes
WISP-22	Maintain continuous threat monitoring OR conduct annual penetration testing supplemented by bi-annual vulnerability scans.	High	☐ Met ☐ Not Met ☐ N/A	Pen-Test / Vulnerability Report

WISP-23	Maintain a written Incident Response Plan (IRP) detailing containment, forensic investigation, and recovery steps.	High	☐ Met ☐ Not Met ☐ N/A	Approved IRP Playbook
WISP-24	Document breach reporting procedures for immediate IRS Stakeholder Liaison notice and 30-day FTC notification.	High	☐ Met ☐ Not Met ☐ N/A	Breach Notification Matrix
WISP-25	Conduct an annual tabletop exercise / workflow drill for FTC 500+ consumer breach reporting (if >= 5,000 consumers).	Low	☐ Met ☐ Not Met ☐ N/A	Tabletop Drill After-Action Note

Audit Completion & Sign-Off

Qualified Individual Signature:	_____ Date: _____
Managing Partner / Owner Signature:	_____ Date: _____