[ WOLF TECH IT SOLUTIONS · SOUTH FLORIDA ]

# WISP Starter Guide

A plain-English overview of Written Information Security Plans, IRS & FTC safeguards, and the cybersecurity checklists every tax professional and small business should review.

**Free Educational Resource**

Edition 2026.01

wolftechitsolutions.com · (786) 373-5311 · Miami, FL

[ SECTION 01 ]

## What Is a WISP?

A Written Information Security Plan (WISP) is a documented set of administrative, technical, and physical safeguards a business uses to protect sensitive client and employee information. It explains who is responsible for security, what data you handle, how you protect it, and what happens when something goes wrong.

**WHY YOUR WISP MATTERS**

- IRS Publication 4557 & 5708 — tax professionals are required to have a written data security plan to maintain a PTIN.
- FTC Safeguards Rule — financial institutions (which includes most tax preparers) must implement a written information security program.
- Client trust — a WISP demonstrates you take confidentiality seriously and gives staff a clear playbook to follow.

[ SECTION 02 ]

## Why IRS & FTC Safeguards Matter

Tax and accounting firms hold some of the most attractive data on the market: Social Security numbers, prior-year returns, banking details, and W-2s. Both the IRS and the FTC have responded with explicit written-plan requirements. The goal isn't paperwork — it's making sure a real plan exists before an incident, not after.

| Framework | What It Requires |
|---|---|
| IRS Pub. 4557 / 5708 | Written security plan, designated security lead, documented safeguards, and ongoing employee training. |
| FTC Safeguards Rule | Risk assessments, access controls, encryption, MFA, monitoring, incident response, and vendor oversight. |
| NIST Cybersecurity Framework | Identify, Protect, Detect, Respond, and Recover — the common backbone most modern WISPs map to. |

[ SECTION 03 ]

## Top 10 Common Security Gaps

Patterns we see most often when reviewing small firms in South Florida.

| | | |
|---|---|---|
| 01 | No designated security lead | Nobody owns the program, so nothing gets reviewed or updated. |
| 02 | Shared or reused passwords | One compromised password unlocks email, tax software, and bank logins. |
| 03 | MFA not enforced everywhere | MFA on email but not on remote access, tax software, or admin accounts. |
| 04 | Unpatched workstations and servers | Missing OS, browser, and tax-software updates for weeks or months. |
| 05 | No real backup test | Backups exist but nobody has ever tried to restore them. |
| 06 | Flat network | Guest Wi-Fi, staff workstations, and servers all on the same LAN. |
| 07 | Email without phishing protection | Standard inbox filters only — no link rewriting or attachment sandboxing. |
| 08 | Sensitive files in personal cloud | Returns or PII in personal Dropbox, Gmail drafts, or USB drives. |
| 09 | No documented incident response | When something happens, the team improvises under pressure. |
| 10 | No vendor security review | Outsourced bookkeepers, IT, and SaaS tools have access with zero oversight. |

[ SECTION 04 ]

## IRS Security Six Checklist

The six baseline protections the IRS recommends for every tax professional.

- [ ] Anti-virus software
  Reputable endpoint protection installed and auto-updating on every device.

- [ ] **Firewalls**
  A properly configured firewall between your network and the internet.
- [ ] **Two-factor authentication**
  Enabled on email, tax software, cloud storage, and remote access.
- [ ] **Backup software / services**
  Automated daily backups stored off-site or in the cloud, and tested.
- [ ] **Drive encryption**
  Full-disk encryption (BitLocker / FileVault) on laptops and workstations.
- [ ] **Virtual Private Network (VPN)**
  Encrypted tunnel for remote work — never use public Wi-Fi unprotected.

**[ NEXT STEP ]**

## Not sure where you stand on the Security Six?

A 30-minute readiness review tells you exactly which items are in place, which need work, and what to prioritize first.

**Schedule a WISP Readiness Review »**

wolftechitsolutions.com/contact · (786) 373-5311

[ SECTION 05 ]

# Basic Cybersecurity Readiness Scorecard

Rate your firm honestly on each item: 1 = not started, 3 = partially in place, 5 = fully implemented and documented.

| | | | | | |
|---|---|---|---|---|---|
| We have a written, dated WISP reviewed in the last 12 months. | 1 | 2 | 3 | 4 | 5 |
| A specific person is named as our security / data lead. | 1 | 2 | 3 | 4 | 5 |
| We maintain an inventory of devices, software, and sensitive data. | 1 | 2 | 3 | 4 | 5 |
| MFA is enforced on email, tax software, and remote access. | 1 | 2 | 3 | 4 | 5 |
| Endpoint protection is installed and centrally monitored. | 1 | 2 | 3 | 4 | 5 |
| Backups run daily, are stored off-site, and were tested in the last 90 days. | 1 | 2 | 3 | 4 | 5 |
| Staff complete security awareness training at least annually. | 1 | 2 | 3 | 4 | 5 |
| We have a written incident response plan with clear roles. | 1 | 2 | 3 | 4 | 5 |
| Vendor access (IT, bookkeepers, SaaS) is reviewed at least yearly. | 1 | 2 | 3 | 4 | 5 |
| Old client data is purged or archived on a defined schedule. | 1 | 2 | 3 | 4 | 5 |

**HOW TO READ YOUR SCORE**

40–50 Strong foundation. Focus on testing and documentation.
25–39 Real gaps. Build a 90-day plan to close the weakest items.
Below 25 High risk. Prioritize MFA, backups, and a written WISP now.

[ SECTION 06 ]

## Phishing Protection Checklist

Email is still the #1 way attackers get in. Cover these basics first.

- [ ] Advanced email filtering with link rewriting and attachment sandboxing.
- [ ] External-sender warning banner on all inbound email.
- [ ] DMARC, SPF, and DKIM configured on your sending domain.
- [ ] Quarterly phishing simulations for all staff.
- [ ] Documented process for reporting suspicious email (one click or one address).
- [ ] Wire-transfer and banking-change requests require voice verification.
- [ ] Annual training that covers gift-card, invoice, and CEO-impersonation scams.

[ SECTION 07 ]

## Multi-Factor Authentication (MFA) Checklist

If you do nothing else this quarter, finish this list.

- [ ] MFA enforced on all email accounts (staff, owners, shared inboxes).
- [ ] MFA on tax preparation and accounting software.
- [ ] MFA on cloud storage (OneDrive, Google Drive, Dropbox, etc.).
- [ ] MFA on remote desktop, VPN, and any admin portals.
- [ ] App-based authenticators or hardware keys preferred over SMS.
- [ ] Recovery codes stored in a password manager, not in email.
- [ ] Process to remove MFA / accounts within 24 hours of staff departure.

[ NEXT STEP ]

### Want a second pair of eyes on your stack?

We run a no-cost readiness review covering MFA, email, backups, and endpoint coverage — and send you a short written summary.

**Schedule a WISP Readiness Review »**

wolftechitsolutions.com/contact · (786) 373-5311

[ SECTION 08 ]

## Backup Checklist

A backup that has never been restored is a hope, not a backup.

- [ ] Automated daily backups of all critical systems and data.
- [ ] At least one copy stored off-site or in a separate cloud account.
- [ ] Backups are encrypted at rest and in transit.
- [ ] Backup account uses MFA and a unique, strong password.
- [ ] Immutable / versioned backups that ransomware cannot overwrite.
- [ ] Documented retention schedule (e.g., 30 / 90 / 365 days).
- [ ] Full restore test completed in the last 90 days.

[ SECTION 09 ]

## Short Incident Response Checklist

The first 60 minutes decide how bad an incident gets. Plan them now.

- [ ] Named incident lead and after-hours contact tree.
- [ ] Step-by-step playbook for suspected phishing, malware, and lost devices.
- [ ] Pre-identified outside help: IT / MSSP, cyber insurance, legal counsel.
- [ ] Client / staff notification templates ready to send.
- [ ] Process to preserve logs and evidence before wiping devices.
- [ ] Post-incident review documented within 30 days, with corrective actions.

[ NEXT STEP ]

## Ready to turn this checklist into a real, written WISP?

Wolf Tech IT Solutions builds customized WISPs for tax, accounting, legal, and medical practices across Miami-Dade, Broward, and Palm Beach. Educational review first — engagement only if it's a fit.

**Schedule a WISP Readiness Review »**

wolftechitsolutions.com/contact · (786) 373-5311

---

### REFERENCES


- IRS Publication 4557 — Safeguarding Taxpayer Data
- IRS Publication 5708 — Creating a Written Information Security Plan
- FTC Safeguards Rule (16 CFR Part 314)
- NIST Cybersecurity Framework


### DISCLAIMER