

WISP Readiness Checklist

Gills IT World LLC

For tax preparers and accounting offices: FTC Safeguards Rule (16 CFR 314) and IRS guidance

Veteran-owned security, Holiday FL

Paid tax preparers are covered by the FTC Safeguards Rule and must keep a written information security plan (WISP). Check each item that is **true and documented** today, not just planned. [small-firm exempt](#) marks items that do not apply if you hold data on fewer than 5,000 consumers (16 CFR 314.6).

PEOPLE AND PLAN

- | | |
|---|--------------|
| ☐ A named Qualified Individual oversees the security program (can be an outside provider, but a senior person at your firm still oversees them) | 314.4(a) |
| ☐ A written WISP exists and matches how the office actually works (IRS sample: Pub 5708) | IRS Pub 5708 |
| ☐ Written risk assessment of where client data lives and what could go wrong small-firm exempt | 314.4(b)(1) |
| ☐ Staff get security awareness training, updated for current risks (phishing, fake IRS and client emails) | 314.4(e)(1) |

CONTROLS THAT MUST ACTUALLY BE TURNED ON

- | | |
|---|-------------|
| ☐ MFA for anyone accessing any system with client data: email, tax software, client portal, remote access, cloud storage | 314.4(c)(5) |
| ☐ Client data encrypted at rest (laptops, servers, backups) and in transit over external networks (portal, email attachments) | 314.4(c)(3) |
| ☐ Each person can reach only the client data their job needs; former staff removed promptly | 314.4(c)(1) |
| ☐ An inventory of the devices, systems, software and people that touch client data | 314.4(c)(2) |
| ☐ User activity is logged and watched for unauthorized access | 314.4(c)(8) |
| ☐ Client data securely disposed of within 2 years of last use, unless retention is required | 314.4(c)(6) |
| ☐ Changes to systems follow a simple change procedure | 314.4(c)(7) |

TESTING AND VENDORS

- | | |
|--|-------------|
| ☐ Key controls are tested or monitored regularly | 314.4(d)(1) |
| ☐ Continuous monitoring, or an annual penetration test plus vulnerability scans every 6 months small-firm exempt | 314.4(d)(2) |
| ☐ Vendors that touch client data (tax software host, IT provider, cloud storage) are chosen with care, required by contract to protect it, and reviewed periodically | 314.4(f) |

WHEN SOMETHING GOES WRONG

- | | |
|--|------------------------|
| ☐ Written incident response plan: who does what, who you call, how you recover small-firm exempt | 314.4(h) |
| ☐ You know the deadlines: FTC notice within 30 days if 500+ consumers are affected; Florida Attorney General within 30 days if 500+ Floridians are affected | 314.4(j); F.S. 501.171 |
| ☐ You know to report client data theft to your IRS Stakeholder Liaison and state tax agency | IRS guidance |
| ☐ The Qualified Individual reports in writing at least yearly to the owner or partners small-firm exempt | 314.4(i) |

Where most offices fall short: the plan says MFA and encryption are on everywhere, but one tax software login, the client portal, or a backup drive is not. After a breach, that gap between the plan and reality is the first thing anyone asks about. When renewing your PTIN, you confirm (Form W-12, line 11) that you know a WISP is required by law.

Gill, Gills IT World LLC: WISP in a Week, \$995 flat, plan written and controls verified

gill@gillsitworld.com · gillsitworld.com

General information, not legal advice. Sources: 16 CFR 314.4 and 314.6 (ecfr.gov); IRS Pub 5708 and 4557; IRS Instructions for Form W-12; Florida Statutes 501.171.