

WISP readiness checklist for tax and accounting firms

28 yes or no questions built from the FTC Safeguards Rule (16 CFR 314) and the IRS Security Six. Check each item that is true at your firm today, then count your checks. Items marked "5,000+ consumers" are not required for firms holding information on fewer than 5,000 consumers, though insurers and clients often expect them.

People and program

- | | | |
|--------------------------|---|------------------------------|
| ☐ | 1. One named person is responsible for your security program, your Qualified Individual. | FTC 314.4(a) |
| ☐ | 2. Your WISP is written for your firm, not an unmodified template, and staff know where to find it. | IRS Pub 5708 |
| ☐ | 3. Your WISP was reviewed and updated in the last 12 months. | IRS IR-2026-92 |
| ☐ | 4. Everyone who touches client data had security training this year, and you kept a record. | FTC 314.4(e) |
| ☐ | 5. You have a written risk assessment that lists your risks and how you handle each one. | Required at 5,000+ consumers |

Access

- | | | |
|--------------------------|--|-----------------|
| ☐ | 6. Multifactor authentication protects every system with client data: email, tax software, portals, cloud storage and remote access. | FTC 314.4(c)(5) |
| ☐ | 7. Every person has their own login. No shared accounts or shared passwords. | FTC 314.4(c)(1) |
| ☐ | 8. People only have the access their job needs, and you review it at least once a year. | FTC 314.4(c)(1) |
| ☐ | 9. When someone leaves, their access is removed the same day. | FTC 314.4(c)(1) |

Devices and network

- | | |
|---|-----------------------------------|
| ☐ 10. Antivirus or endpoint detection runs on every computer. | IRS Security Six |
| ☐ 11. A firewall protects the office network and each device. | IRS Security Six |
| ☐ 12. Laptops and desktops use full drive encryption. | IRS Security Six, FTC 314.4(c)(3) |
| ☐ 13. Remote work goes through a VPN or another secure remote access tool. | IRS Security Six |
| ☐ 14. Updates and patches are applied on a schedule. | FTC 314.4(c)(7) |
| ☐ 15. You keep an inventory of devices, systems and where client data is stored. | FTC 314.4(c)(2) |

Client data

- | | |
|---|------------------|
| ☐ 16. Backups run automatically, a copy is kept offsite or locked from changes, and you have test restored them this year. | IRS Security Six |
| ☐ 17. Clients send and receive files through a secure portal, not email attachments. | FTC 314.4(c)(3) |
| ☐ 18. Client data is encrypted whenever it travels over the internet. | FTC 314.4(c)(3) |
| ☐ 19. Client data you no longer need is securely destroyed, generally within two years of last use. | FTC 314.4(c)(6) |
| ☐ 20. You have a written rule for AI tools, including no client data in personal AI accounts. | Best practice |

Vendors

- | | |
|--|--------------|
| ☐ 21. You have a list of every vendor that can access client data, including IT support and software providers. | FTC 314.4(f) |
| ☐ 22. Your contracts require those vendors to protect the data, and you review them periodically. | FTC 314.4(f) |

Detect and respond

- | | |
|--|------------------------------|
| ☐ 23. Activity on systems that hold client data is logged and monitored. | FTC 314.4(c)(8) |
| ☐ 24. You have a written incident response plan with contacts for your IRS Stakeholder Liaison, state tax agencies, insurer and attorney. | Required at 5,000+ consumers |
| ☐ 25. You know the FTC rule: a breach of unencrypted data on 500 or more consumers must be reported to the FTC within 30 days of discovery. | FTC notice rule |
| ☐ 26. You run vulnerability scans every six months and a penetration test each year, or monitor your systems continuously. | Required at 5,000+ consumers |
| ☐ 27. Your Qualified Individual gives the owners a written security report at least once a year. | Required at 5,000+ consumers |
| ☐ 28. You have cyber insurance, and your application answers about MFA and backups are still true. | Best practice |

Your score: ____ of 28

24 or more: a solid program. Keep the evidence current and review it every year.

15 to 23: real gaps. Most are fixable in a few weeks, outside busy season.

Under 15: your WISP probably would not hold up to an insurer, examiner or breach. Start now.

Want a second set of eyes? Book a fixed-price WISP and Security Six Diagnostic at sunesisservices.com/book or email hello@sunesisservices.com.

Sources

FTC Safeguards Rule, 16 CFR 314 (summary by Bradley):

<https://www.bradley.com/insights/publications/2023/06/complying-with-the-ftcs-amended-safeguards-rule>

16 CFR 314.6, small institution exceptions: <https://www.federal-regs.com/title/16/part-314/314.6/>

FTC breach notice requirement (summary by Venable):

<https://www.venable.com/insights/publications/2023/11/data-breach-notice-requirement-added>

IRS Tax Tip 2026-72:

<https://www.irs.gov/newsroom/fall-has-arrived-but-the-security-summit-summer-series-information-is-relevant-year-round>

IRS IR-2026-92, August 18, 2026: <https://www.irs.gov/newsroom/irs-security-summit-remind-tax-pros-they-need-a-written-information-security-plan-to-protect-client-data>