



IRS, Security Summit remind tax pros they need a Written Information Security Plan to protect client data

“Protect Your Clients; Protect Yourself” series highlights federal security requirements.

IR-2026-92, Aug. 18, 2026

WASHINGTON — The Internal Revenue Service and Security Summit partners today reminded tax professionals to protect client data with a Written Information Security Plan.

Federal law requires tax and accounting professionals to create and maintain a Written Information Security Plan to help protect client information from identity thieves and data breaches. The IRS offers publications and other resources to help tax professionals develop, test, and update these plans.

This is the third installment of a five-part summer news release series focused on tax professional security. The “Protect Your Clients; Protect Yourself” campaign provides timely tips to help protect sensitive taxpayer data and businesses from identity theft.

Security tips and the WISP requirement are also a key focus of the Nationwide Tax Forum, held this summer in cities across the U.S. The forums continue this week in New York City, with remaining events in Orlando and San Diego.

What tax pros should know about WISPs

The Gramm-Leach-Bliley Act requires all financial institutions to protect customer data. Under this law, tax and accounting professionals are considered financial institutions and must implement a data security plan. As a part of the plan, the Federal Trade Commission requires each firm to:

- Designate one or more employees to coordinate the information security program.
- Identify and assess risks to customer information in relevant areas of the company's operation and evaluate the effectiveness of safeguards.
- Create, implement and regularly monitor and test security safeguards.
- Select service providers that can maintain appropriate safeguards and ensure their contracts require compliance.

The basics of a WISP

A good WISP focuses on three areas:

- Employee management and training
- Information systems
- Detecting and managing system failures

IRS offers WISP tools and resources

[Publication 5708, Creating a Written Information Security Plan for Your Tax & Accounting Practice](#) provides a template to help tax professionals, especially smaller practices, develop a WISP. The publication guides users through starting a plan, including understanding security compliance requirements and professional responsibilities.

Tax professionals are legally required to have a written, accessible plan and should review, test, and update it regularly. Firms should make adjustments based on changes in operations or results from security testing and monitoring.



As part of a security plan, the IRS also recommends that tax professionals develop a data theft response plan, including contacting their [IRS Stakeholder Liaison](#) to report a security incident. Tax professionals can also share information with the appropriate state tax agency by visiting the Federation of Tax Administrators' webpage: [Report a Data Breach](#).

Tax professionals should understand security event reporting requirements under the [FTC's Safeguards Rule](#) as part of their overall information and data security plan. Under the rule, covered financial institutions must report certain security events affecting 500 or more people to the FTC, generally within 30 days of discovery.

Additional resources

- [Publication 5709, How to Create a Written Information Security Plan for Data Safety](#).
- [Publication 5293, Data Security Resource Guide for Tax Professionals](#), which provides an overview and resources about how to avoid data theft.
- Tax professionals can also get help with security recommendations by reviewing IRS [Publication 4557, Safeguarding Taxpayer Data](#), and the IRS's [Identity Theft Information Page for Tax Professionals](#).
- [Small Business Information Security: The Fundamentals](#), by the National Institute of Standards and Technology, provides additional information for small businesses.

Tax professionals should also stay connected to the IRS through subscriptions to [e-News for tax professionals](#) and IRS [social media sites](#).