

Securing the Tax Practice: WISP, IRS Pub 4557, and Practical Controls

Credits 2.0	Field of Study Taxes	Course Category General	Level Intermediate
----------------	-------------------------	----------------------------	-----------------------

COURSE DESCRIPTION

The IRS requires every professional tax preparer to have a Written Information Security Plan (WISP), but a document sitting in a drawer doesn't stop a data breach. This session focuses on turning regulatory requirements into a functional security posture. The firm needs to understand how IRS Publication 4557 translates to daily operations, from the way staff logs into software to how they vet third-party vendors. The discussion moves beyond the legal mandate to address the actual tools that protect client data, including the transition to passkeys and the necessity of encrypted communications. Finally, the session covers the critical steps a firm must take when a security incident occurs, ensuring the practice meets its reporting obligations while minimizing damage to its reputation.

LEARNING OBJECTIVES

- Identify the mandatory components of a Written Information Security Plan as required by the IRS.
- Compare traditional multi-factor authentication methods against modern passkey implementations for firm access.
- Evaluate the security protocols of cloud-based vendors during the due diligence process.
- Outline the immediate procedural steps required following a data breach or unauthorized access to client returns.
- Apply encryption standards to common communication channels used within a tax practice.

MAJOR TOPICS

- IRS Publication 4557 and the WISP mandate
- Access control strategies for remote and hybrid teams
- Transitioning from passwords to MFA and passkeys
- Vendor risk management and data processing agreements
- Hardware security and device management for tax staff
- Client data encryption in transit and at rest
- Incident response planning and reporting requirements

WHAT YOU'LL WALK AWAY WITH

- You'll draft a functional Written Information Security Plan that meets every IRS requirement.
- You'll replace vulnerable passwords with passkeys and modern authentication to lock down firm access.
- You'll vet your cloud vendors using a specific security checklist to ensure they protect your data.
- You'll set up encrypted communication channels that keep client returns private during every exchange.
- You'll follow a clear step-by-step response plan to handle any data breach or security incident.

QUESTIONS

Is this course only for large firms with dedicated IT departments?

No. Solo practitioners and small firm administrators will find the material particularly useful because it focuses on practical tools you can manage yourself. We focus on the specific steps any tax professional must take to stay compliant.

Do I need to be a security expert to understand the technical sections?

You don't. While the course is at an intermediate level, I explain concepts like passkeys and encryption standards in plain language that relates to your daily tax work. We're looking at how these tools fit into your office, not how to write the code behind them.

Does this course provide a template for the WISP?

We identify all the mandatory components required by IRS Publication 4557 so you can build a plan that fits your specific practice. You'll learn what needs to be in the document to satisfy a regulatory audit.

Will we cover hardware security for employees who work from home?

Yes. The session specifically addresses access control strategies for remote and hybrid teams, including how to manage devices that aren't physically in your office. We'll look at keeping data safe regardless of where your staff is sitting.

What kind of prior knowledge should I have before starting?

You should have a general familiarity with how a tax firm operates and basic IRS compliance requirements. There's no advanced preparation needed, but you'll get the most out of this if you're already handling client data regularly.

A NOTE FROM THE AUTHOR

I started this project because I noticed too many colleagues treating their security plans as a chore to be filed away rather than a shield for their business. I wrote this for the practitioners who feel overwhelmed by technical jargon but know they need to keep their clients safe. We're going to turn these cold IRS mandates into a set of practical habits that actually work for your firm.

ADDITIONAL INFORMATION

- **Who Should Attend:** Tax partners, solo practitioners, firm administrators, and IT managers responsible for tax data security.
- **Prerequisites:** General familiarity with tax firm operations and IRS compliance requirements.
- **Advanced Preparation:** None
- **Tags:** cybersecurity, irs compliance, wisp, data privacy, tax technology
- **Course ID:** 2200
- **Short Name:** Securing the Tax Practice: WISP, IRS Pub 4557, and Practical Controls

SECURING THE TAX PRACTICE: WISP, IRS PUB 4557, AND PRACTICAL CONTROLS

