rightworks

eBook

How to get your written information security plan right

Your accounting firm must have a written information security plan, or a WISP. Yes, it's a good idea to have one, and yes, it can save you from a devastating cyberattack. But beyond all that, if you prepare even one tax return as part of your practice, you need to have a WISP in place.

The IRS **states it very simply**: "Federal law requires all professional tax preparers to create and implement a data security plan."

This requirement has teeth, too. Your firm's tax preparers must attest on their form W-12 each year that they understand the need for a security plan to renew their Preparer Tax Identification Number (PTIN). So, if you want to practice accounting, you have to have a security plan. There are other regulations that go beyond PTIN renewal as well.

But it's just a matter of scribbling down a few promises to use antivirus software and not share clients' phone numbers, right? Oh, no. Creating a WISP that passes muster is a massive chore. One cybersecurity expert who spoke to the author of this guide said he spent a full 40-hour week creating a WISP for a four-person accounting firm.

You can try to create a WISP yourself. Before you do, though, you should know that it will take time and resources beyond what most firms can reasonably commit.

How can you comply, then? The bottom line is: You're going to need help.

Is a written information security plan really a requirement?

As with most issues involving legislation and government agencies, the WISP requirement isn't as simple as it could be. It does, however, exist. How and where? Hang on for the ride.

First, there's the PTIN issue. If you want to renew your PTIN, you must state on Question 11 of IRS form W-12 that you understand you must have a data security plan in place as a paid tax preparer. You don't necessarily have to show your plan to protect client data, but you must acknowledge that you know you're supposed to have one.

What's the potential penalty if you don't have a WISP and say you do? Well, you're committing perjury and could lose your license. So, PTIN renewal effectively requires a WISP. And again, even the IRS itself uses the phrase, "Federal law requires all professional tax preparers to create and implement a data security plan." There's no real ambiguity there.

This isn't necessarily something new; similar requirements have existed for decades. The Gramm-Leach-Bliley Act (GLBA) required businesses to explain information-sharing practices and **safeguard sensitive data** back in 1999. The GLBA doesn't specifically mention a written information security plan, but a product of it, the **FTC Safeguards Rule**, definitely does.

Your firm is almost assuredly subject to the FTC Safeguards Rule. In some cases, firms with fewer than 5,000 records are **required to comply with parts of the Safeguards Rule** as well. Your firm should look into your compliance status. To be clear, that's not 5,000 clients; it's 5,000 records. For instance, an item such as a non-public client email address or a receipt showing a client expenditure with a business partner is a record. The numbers add up quickly—which means yes, a WISP is necessary.

> **"Federal law requires all professional tax preparers to create and implement a data security plan."**

Why a WISP isn't easy to create

The IRS doesn't technically have a list of requirements for a WISP, but it does have certain elements the agency thinks should be part of a compete WISP. **The IRS also has a sample WISP that demonstrates how complicated creating a written plan can be**. If you want to skimp on your WISP and try to get by, that's a path fraught with peril. It's a bad idea from a cybersecurity perspective, and you're unlikely to stay in the good graces of the IRS should you suffer a security incident.

What's more, you risk running afoul of the FTC Safeguards Rule, which has a long and complex list of requirements that firms must meet to comply. The Safeguards Rule requires you to create a WISP that includes, among other things, a **complete inventory** of all the information you have and where you have it stored. (Yes, that includes file cabinets and thumb drives.)

But the real kicker is that just writing a WISP isn't enough for the FTC. You also have to **implement your plan**. The WISP itself can require a full work week to create, even for a small firm. Implementing the WISP is an enormous and ongoing task. Components of the Safeguards Rule can and do change; the **deadline to comply** with the latest set of changes was June 2023. Plus, the FTC requires that you periodically update and test your plan.

While the IRS requirements around WISP content are less iron-clad, the agency does have a long and detailed list of components that it believes firms should have in a WISP. Fortunately, the agency provides a guide to help your firm write a WISP. Unfortunately, it's **29 pages long** and not simple. Still, if the IRS strongly suggests specific elements be included in a WISP, it's a good idea for your firm to include them.

What you need to do to create a WISP

Of course, the best reason to create a written information security plan is to protect your clients' data. Having a cybersecurity plan does a lot more than check a compliance box. It helps you ensure that your firm can survive a cyberattack. One study revealed that only 29% of firms would **survive for more than a week** after a ransomware attack. And yet the same study showed that 14% of firms do not have a written incident response plan—which is similar to and really should be a component of a WISP.

> **One study revealed that only 29% of firms would survive for more than a week after a ransomware attack.**

Another study showed that 51% of US businesses suffered a cyberattack in 2023. In 20% of those cases, the very existence of the business **hung in the balance**. Those businesses survived, but their "solvency was materially threatened" after the attack. Given how quickly a cyberattack can destroy your firm, having a plan in place to avoid and mitigate one is just a smart practice.

Plus, if you don't have an adequate security plan and you do suffer a cyberattack, you're less likely to be able to defend yourself from client lawsuits and other legal actions. So, what do you need to create a WISP that satisfies FTC Safeguards Rule requirements and looks good to the IRS and clients?

This is an oversimplification, but it will give you an idea of how much work you need to put in. Your WISP needs to include some critical components:

Stated objective and purpose. This is fairly simple. You want to protect your clients' Personal Identifiable Information, or PII, which is (not super helpful) basically the same as PPI, or Private Personal Information. Whatever you call it, it includes a lot of information.

The US Department of Labor **offers a relatively simple overview** of PII as "information (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification."

Put all those things in a list, though, and that list will include **just about any piece of client information** you can think of, from passport and driver's license numbers to gender and ethnicity. You have a responsibility to secure pretty much anything a client discloses to you.

A risk assessment and results. Now things get complicated. You must be able to identify every piece of PII you have, how you're storing it and how you're protecting it. That means looking into every computer, server, thumb drive, external hard drive and file cabinet—yes, paper counts—and listing which ones contain client data. Email counts, too, as do any software as a service applications and simple cloud services where you might be storing client data.

You have to show in your WISP that you can protect client data wherever it's stored, even if the same data is stored in two different places. If you have paper files in a cabinet, you need to prove that you can protect them from, say, a cleaning contractor who might clean your office at night, thereby having access to client data.

You're required to determine the level of risk for each piece of your data—and how you plan to protect it. Demonstrating the ability to protect client data in electronic formats will be even more complex and difficult. If you're storing data in multiple places and formats, this could be a time-consuming chore prone to errors. And remember, you're dealing with all your data, not just 2023 tax returns.

A list of all your security software and services. To go along with knowing where your data is, you need to know exactly what you have protecting it. You need to take stock of all your security applications, from antivirus to multifactor authentication (MFA). You might find that you're not quite sure how you're protecting your data... and that you don't have enough protection in place.

What are you doing with MFA? The **IRS says firms should have** this technology in place as part of the agency's "Security Six" cybersecurity protections. These are the types of questions you need to know the answers to.

The deep dive into your security infrastructure is likely to be both time-consuming and revealing, but it's non-negotiable for meeting basic security requirements.

Other key components. As if all of that wasn't enough, there's a lot more to think about when creating a WISP. These elements are no less important than those already listed. They just don't require quite as much explanation. Nevertheless, you still need:

- **A plan for responding to a data breach.** What will you do if you suffer an attack? How do you get your data back if a cyberattacker steals it? You must document all of that.
- **Security policies for staff and contractors.** Are you providing cybersecurity training for your employees? The FTC Safeguards Rule requires that you do.
- **Policies for monitoring and reviewing the WISP.** You're never done with your WISP. You need to review it periodically, preferably at least every six months. And if government requirements change, your WISP needs to change, too.

Don't try to create a WISP alone

Compliance with the Safeguards Rule requires your firm to have a qualified professional in charge of creating and implementing your security plan. However, most firms don't have anyone like that. It doesn't have to be a full-time employee, but someone must be in charge. Still, that requirement alone is too much for most firms to handle.

Not that it matters that much, though, because the whole process of creating a WISP is far beyond what most firms can take on themselves. Just as most IT professionals couldn't prepare a tax return, most accountants don't have any cybersecurity expertise. Creating a WISP that meets requirements necessitates not only expertise, but also the resources to get the work done.

At a time when most firms are having trouble recruiting and keeping accounting talent, can your firm afford to assign employees—regardless of expertise—to create and manage a security plan? You have clients to serve and a firm to run. Getting bogged down with a project as critical and complex as creating a WISP is very unlikely to be a serious option for your firm. Your clients come to you for accounting expertise. You need to turn to experts to manage cybersecurity.

Again, going without a WISP or trying to fake your way into creating a plan is not feasible. For the sake of your firm, your clients and even your PTIN, you need a WISP—and you need help creating it.

Turn to experts to create your WISP

A cloud provider with a mature security team can serve as the guide you need to create and implement a WISP, as well as to manage the technology required to maintain it. When you let a partner manage security for you, you can get on with running your firm.

Rightworks has more than two decades of experience handling security for accounting firms. With Rightworks, you not only have the designated expert you need to manage your security initiatives, but you also have a whole team that can create, implement, test and maintain your security plan.

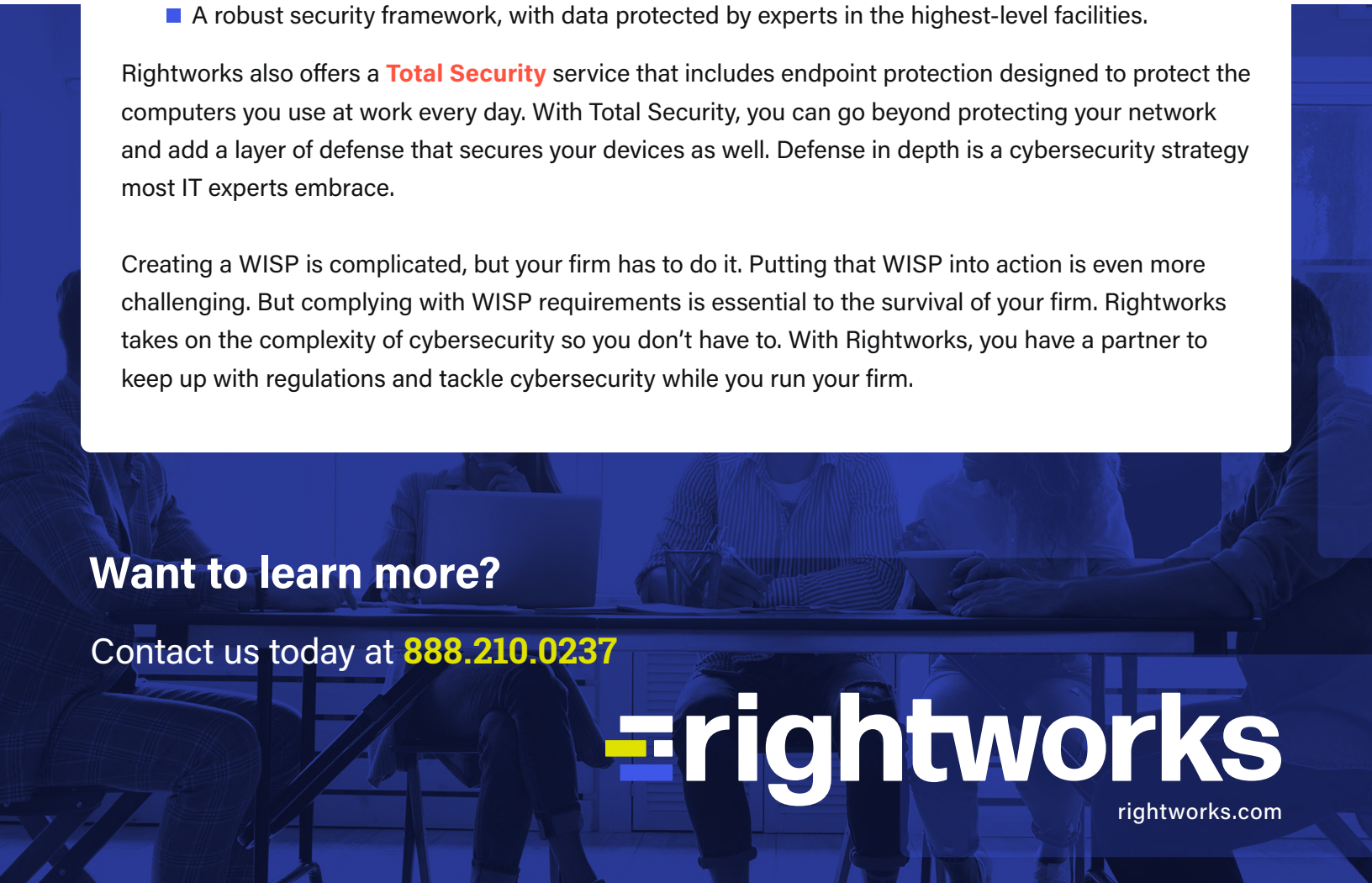
With our dedicated team, Rightworks will provide the help you need to complete your WISP. But Rightworks can also help your firm get the security solutions in place that will fill any gaps in your cybersecurity strategy. And with **OneSpace**, Rightworks can maintain your security infrastructure and protect your clients' data around the clock.

Rightworks provides:

- A team of experts dedicated to your firm who can help you meet security requirements and challenges.
- The highest level of performance, with 99.999% uptime, limitless scalability and fast connectivity.
- A robust security framework, with data protected by experts in the highest-level facilities.

Rightworks also offers a **Total Security** service that includes endpoint protection designed to protect the computers you use at work every day. With Total Security, you can go beyond protecting your network and add a layer of defense that secures your devices as well. Defense in depth is a cybersecurity strategy most IT experts embrace.

Creating a WISP is complicated, but your firm has to do it. Putting that WISP into action is even more challenging. But complying with WISP requirements is essential to the survival of your firm. Rightworks takes on the complexity of cybersecurity so you don't have to. With Rightworks, you have a partner to keep up with regulations and tackle cybersecurity while you run your firm.



Want to learn more?

Contact us today at **888.210.0237**

rightworks

rightworks.com