



eBook

Your guide to creating a **Written Information Security Plan**



Does your business have a written information security plan, or WISP? It should. Here are a few reasons why:

A cyberattack can kill your business. One study showed that 75% of small and midsize businesses (SMBs) would only survive for 3 to 7 days after a ransomware attack. Another revealed that 51% of businesses in the US suffered a cyberattack last year, and 20% of the victims almost went out of business after the attack. (In the words of the survey, their “solvency was materially threatened.”)

That means about 10% of all the businesses in the survey had to fight for their lives after a breach. And those were the SMBs that survived. Others did not.

Insurance might not pay off on your claim. Cyber insurance is critical for businesses of all sizes. While you don’t need a WISP to have an insurance policy, you might come up empty-handed if you make a claim and don’t have a WISP. In some documented cases, insurance companies have refused to pay damages because the insured party did not have a WISP in place.

You might need to defend your business against liability. Along the same lines as cyber insurance issues, your business could be more likely to be found liable for damages after a cyberattack if you don’t have a WISP in place. Customers and partners that sue are more likely to be able to prove negligence if you don’t have a plan for mitigating attack damage.

Some states require businesses to have WISPs. More than half of US states require businesses to have a WISP or something similar in place. If you do any business outside your own state, you probably already know that state-to-state regulations quickly get complicated and confusing. Requirements around data security are no exceptions.



What is a Written Information

Security Plan, anyway?

You need a WISP not only because you might need to make an insurance claim or defend your business in a lawsuit, but also because the threat of a cyberattack is very real. You need to know both how to prevent one and respond to one. Your customers trust you with their data, just as you trust the companies you buy from and partner with.

As any business owner knows, not having a plan for any initiative or eventuality is a recipe for disaster. The same idea applies to cybersecurity; you don't want to be left not knowing what to do while your business hangs by a thread after an attack. You need to be prepared.

But here's a word of caution: Developing a WISP that can help you avoid or mitigate damage from a cyberattack is not easy. It's not a simple process. 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. It's going to take time and resources beyond what most SMBs can reasonably commit. How can you do it, then? The bottom line is: You'll need help.

What you need to do to create a WISP

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 customers' Personal Identifiable Information, or PII, which is (not super helpfully) 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) 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 includes **just about any piece of customer 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 customer 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 customer data. Email counts, too, as do any software as a service applications and simple cloud services where you might be storing customer data.

You have to show in your WISP that you can protect 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 sensitive 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 customer data in electronic formats will prove to 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.

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. You might find that you're not sure exactly how you're protecting your data...and that you don't have enough protection in place.

For instance, do you use an anti-phishing toolbar? Would you know if you did? If you don't, you should. The same goes for multifactor

identification (MFA), a technology that's critical for stopping phishing and ransomware attacks. The deep dive into your security infrastructure is likely to be both time-consuming and revealing, but it's non-negotiable for creating a useful WISP.

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? When and how do you inform your customers? You must document all of that.
- **Security policies for staff and contractors.** Are you providing cybersecurity training for your employees? You should. Most cyberattacks start with human error, so your employees are your best defense against a data breach.
- **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.



Don't try to create a WISP alone

The bottom line is that the whole process of creating a Written Information Security Plan is far beyond what most SMBs can take on themselves. Just as most IT professionals couldn't do what you do for customers, most SMB owners don't have any cybersecurity expertise. Creating a WISP necessitates not only expertise but also the resources to get the work done.

At a time when many businesses are having trouble recruiting and keeping talent, can you afford to assign employees—regardless of expertise—to create and manage a security plan? You have a business to run, which is difficult enough without taking on extra tasks. Getting bogged down with a project as critical and complex as creating a WISP is very unlikely to be a serious option for your business. Your customers come to you for products and services they can't get anywhere else. You need to turn to experts to create a WISP.



Turn to experts to create your Written Information Security Plan

The right technology partner can serve as the guide you need to create and implement a Written Information Security Plan, 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 business.

Rightworks has more than two decades of experience handling security for businesses of all kinds. With Rightworks, you not only have the experts you need to manage your security initiatives, but you also have a partner that can help you create, implement, test and maintain your security plan.

Rightworks will provide the help you need to complete your WISP. But Rightworks can also help your business get the security solutions in place that will fill any gaps in your cybersecurity strategy. And with **OneSpace**, Rightworks can protect your customers' data around the clock.

Rightworks provides:

- Security experts who can help you meet the challenge of developing and implementing a WISP.
- 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.

Plus, **Rightworks Total Security** adds device protection and enhanced backups, as well as security awareness training so your employees will know how to avoid cyberthreats.

Creating a WISP is complicated, but every business should have one. Putting that WISP into action is even more challenging. Rightworks takes on the complexity of cybersecurity so you don't have to. With Rightworks, you have a partner on your side to tackle cybersecurity while you run your business.

Want to learn more?

Contact us today at **888.210.0237**

