How to Create a **Written Information Security Plan** for Data Safety

WISP

IRS

With data security incidents continuing, tax professionals must have current written information security plans or WISPs.

Federal law, enforced by the Federal Trade Commission, requires professional tax preparers to create and maintain a written data security plan.

Having a WISP protects businesses and clients while providing a blueprint of action in the event of a security incident. In addition, a WISP can help if other events occur that can seriously disrupt a tax professional's ability to conduct normal business, including fire, flood, tornado, earthquake and theft.

The Security Summit developed a plain language sample plan that tax pros can use for guidance in making their own WISP. The **sample plan** is available on IRS.gov.

A security plan should be appropriate to the company's size, scope of activities, complexity and the sensitivity of the customer data it handles.

Developing a WISP

A good **WISP** should identify the risks of data loss for the types of information handled by a company and focus on three areas:

1. Employee management and training.
2. Information systems.
3. Detecting and managing system failures.

Understanding post-breach responsibilities is important in creating a WISP. A good resource is the **FTC's Data Breach Response Guide.**

As a part of the plan, the FTC requires each firm to:

- Designate one or more employees to coordinate its information security program.
- Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling those risks.
- Design and implement a safeguards program, and regularly monitor and test it.
- Select service providers that can maintain appropriate safeguards.
- Evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Maintaining a WISP

A good security plan requires regular maintenance and upkeep. Here are tips to keep a WISP effective:

- Once completed, tax professionals should keep their WISP in a format that others can easily read, such as PDF or Word. Making the WISP available to employees for training purposes is also encouraged. Storing a copy offsite or in the cloud is a recommended best practice in the event of a physical disaster.
- It is important to understand that a WISP is intended to be an evergreen document. It is important to regularly review and update any security plan, along with adjusting the plan to accommodate changes to the size, scope and complexity of a tax professional's business.
- As part of a security plan, the IRS also recommends tax professionals create a data theft response plan, which includes contacting their **IRS Stakeholder Liaison** to report a theft. Also see the **FTC data breach response requirements** listed above.

Publication 5709 (11-2022) Catalog Number 93463H Department of the Treasury **Internal Revenue Service** www.irs.gov