Compliance Checklist: Does Your Written Information Security Plan (WISP) Comply with Federal Law?

SmartVault

Updated 2024

Introduction

As an accounting professional, you're legally obligated to protect the sensitive data you handle and ensure it doesn't get into a cybercriminal's hands. This is a large obligation to meet, especially since cyberthreats continue to escalate rapidly. Take simple phishing emails, for example. AI language models have made these scams virtually indistinguishable from legitimate communications.

To safeguard your business and clients' valuable information and maintain client trust, the Federal Trade Commission (FTC) introduced the Safeguards Rule in 2003, requiring paid tax and accounting professionals to develop and implement a comprehensive ***Written Information Security Plan (WISP).***

Failure to comply with the Safeguards Rule and maintain a robust WISP can result in significant legal and financial consequences, not to mention the potential damage to your firm's reputation and business continuity in the event of a data breach.

> This checklist will guide you through the essential components of a WISP, helping you meet regulatory requirements and demonstrate your commitment to data security and customer privacy.

So, What Makes a Strong WISP?

- **Risk assessment and identification of assets and vulnerabilities**
- **Incident response and disaster recovery planning**
- **Implementation of security controls and access management**
- **Ongoing employee training and awareness programs**
- **Regular testing, monitoring, and updating of security measures**

SmartVault

Understand Cybersecurity Basics

Knowledge is key. Before you create new processes, you must understand the basics.

- ☐ Learn general cybersecurity facts and the common ways cybercriminals gain access to data (malware, phishing, man-in-the-middle, ransomware, etc.)
- ☐ Understand your obligations to comply with legal, regulatory, and industry mandates, like the Federal Trade Commission's (FTC) Written Information Security Plan (WISP) requirement, Gramm-Leach-Bliley Act (GLBA), and others
- ☐ Stay updated on cybersecurity threats/risks and regularly review, test, and update your cybersecurity program (see below) to meet the latest recommendations

Evaluate Your Risks and Current Workflows

When you have a general understanding of cybersecurity, you can determine your business's unique risks.

- ☐ Designate at least one employee who is responsible for your cybersecurity program
- ☐ Identify vulnerabilities and risks that are specific to your business, such as unauthorized access, loss of data, and use/disclosure of information
- ☐ Create an inventory of all the devices and hardware your business uses to handle data (i.e., desktop computers, cell phones, routers, printers, etc.), including what you use each for and where they're located
- ☐ List the data your business handles, including both physical, hardcopy data and electronic data
- ☐ Review your Business Continuity Plan to define potential data loss scenarios (i.e., a computer is stolen or hacked, data corrupted, hard copy paper files are destroyed in a fire, etc.) and outline how you monitor, test, and respond to these risks and threats

Risk Assessment Worksheet: How Vulnerable is Your Firm?

Complete this quick risk assessment to identify where your cybersecurity measures are leaving you vulnerable.

Download the Worksheet

Create a Cybersecurity Program

Take what you learned from the previous steps to create a strong cybersecurity program. Your program should, at a minimum, document everything below.

Data Collection and Retention

- ☐ Identify how much data you store and for how long, where and how you store that data, and who has access to the data
- ☐ Review the flow of data, considering what happens from when you receive the data to when you're ready to store it
- ☐ Document as many details as possible about how your data is cared for and accessed
- ☐ Identify all potential points of failure in your workflow
- ☐ Ensure all data is encrypted during transit and at rest
- ☐ Don't use emails to send or request sensitive data
- ☐ Implement a secure document management system to request, send, and store data in the cloud

Data Backup

- ☐ Identify what data you need to back up (the information your business couldn't function without)
- ☐ Keep your backup data separate from your computer or network by using an external hard drive, USB, or, ideally, the cloud
- ☐ Consider a vendor for cloud storage that provides automated data backup, follows strict security measures, and helps ensure you don't lose your data to a disaster, cyberattack, or human error

Destroying or Deleting Data

- ☐ Destroy or remove data from computers, CDs, USBs, cells, and other electronic devices before you dispose of them
- ☐ Shred paper documents that contain sensitive information

Data Disclosure

- ☐ List the third-party companies that access your data and why
- ☐ Define requirements for third-party data access (i.e., Two-Factor Authentication, password requirements, etc.)
- ☐ Describe how you evaluate and confirm that third parties meet privacy standards
- ☐ Comply with unauthorized disclosure regulations applicable to your business

User and Remote Access

- ☐ Set access permissions based on employee roles and ensure your vendors provide strong access control options
- ☐ Require Two-Factor Authentication
- ☐ Create a process for Unsuccessful Login lockouts
- ☐ Develop a remote access policy

Network Protection

- ☐ Define user protocols and requirements:
  - ☐ Require passwords to have at least 12 characters (a mix of letters, symbols, and numbers)
  - ☐ Set passwords to expire regularly and ensure your vendors have appropriate password requirements and policies
  - ☐ Remind employees not to use the same password for multiple devices or accounts
  - ☐ Do not leave passwords or credentials on sticky notes, notebooks, etc.
  - ☐ Consider using a password manager program to track passwords
  - ☐ Require employees to lock computers before stepping away from their desks
  - ☐ Remind employees to report suspicious emails, texts, or phone calls
- ☐ Describe the process for adding new devices or software to your network:
  - ☐ Confirm that all devices meet security requirements
  - ☐ Designate an employee who approves each new software or device
  - ☐ Develop a strategy for preventing staff from downloading risky apps
- ☐ Describe how you monitor computer systems for hackers or unauthorized access
  - ☐ Use firewall protection, anti-virus, anti-malware, and other security software that updates automatically
  - ☐ Ensure third-party vendors automatically install patches that resolve software vulnerabilities
  - ☐ Change the default admin passwords on your routers
  - ☐ Require employees to install updates as needed on their hardware, computers, and devices
  - ☐ Remind employees not to use public wi-fi for work
  - ☐ Track activity across your documents, including who has accessed the data and when

Incident Response

- ☐ Create an incident response team with clear assignments, objectives, and responsibilities
- ☐ Develop a framework that outlines action items and procedures
- ☐ Document information about external resources and how/when to notify the appropriate persons of the data breach, like your staff, customers, the FTC, FBI, local law enforcement, etc.
- ☐ Describe steps to re-secure devices, passwords, network, and data
- ☐ Develop a continuity plan

Ensure Employees Follow Processes

Your staff are your biggest risk when it comes to data breaches. They're also your first line of defense.

- ☐ Develop an employee/contractor training policy:
  - ☐ Create a training program based on your cybersecurity program
  - ☐ Require new staff (full-time and temp workers) to read the cybersecurity program and complete training during onboarding and at least twice throughout the year
  - ☐ Regularly remind employees of your policy and their legal obligation to protect customer data
- ☐ Ensure all employees pass a background check and submit references
- ☐ Develop and implement non-disclosure agreements and privacy guidelines
- ☐ Ensure terminated or separated employees do not continue having access to network and data

On-Demand Webinar

How To Implement a Cybersecurity Plan and Prepare for an Attack

Hear practical guidance on creating a tailored cybersecurity program. You'll learn what systems are critical to run your business and how to reduce the risk of an attack, as well as the implications from a compliance perspective of not having a plan in place.

Watch the Webinar

How to Make Compliance Simpler

Partner with a vendor that takes the responsibility of protecting your information seriously. Built with bank-grade security, SmartVault's document management system and client portal can help you implement required safeguards. Plus, you'll have powerful tech helping you run your business.

Here's how SmartVault helps with compliance:

Access Controls
Set granular access to files and folders, and who can view, create, edit, or delete them. Quickly see who has access and revoke or change their permissions.

Encryption at Rest and Transit
SmartVault automatically encrypts your data in transit and at rest using bank-level standard AES-256 bit encryption.

Multi-Factor Authentication (MFA)
SmartVault has MFA, which requires users to log in with their email address, password, and a verification code.

Information Disposal
Admins can remove a customer's data in just a few steps.

Activity Monitoring
SmartVault automatically tracks all user activity, including when they upload, download, delete, or change a folder, vault, or document. This report is an authoritative record that no one can edit.

Reliable Security
You're responsible for ensuring the data is safe on your selected vendor's software. You can rest assured it is with SmartVault.

Join over 30,000 accounting professionals who confidently protect their data with SmartVault.

Learn more: smartvault.com ►