Written Information Security Program (WISP)

Introduction

A Written Information Security Program (WISP) is a formal document that outlines how an organization protects sensitive information through administrative, technical, and physical safeguards. The concepts of WISP evolved over time through various laws and regulations. Starting in 2021, amendments to the Safeguard Rules and IRS regulations made WISP mandatory for tax professionals. In 2023, the IRS began enforcing WISP requirements for tax professionals as part of the Preparer Tax Identification Number (PTIN) renewal process.

Entities the Program Applies To

A WISP is a structured framework that defines how an organization:

- Identifies and assesses cybersecurity risks
- Implements safeguards to protect sensitive data
- Responds to security incidents
- Ensures compliance with applicable laws and regulations

WISP requirements apply to entities that handle **sensitive personal** or **financial data**, including:

- Tax Professionals (mandated by the IRS)
- Financial Institutions (under GLBA and FTC Safeguard Rule)
- Healthcare Providers (Under HIPAA)
- Insurance companies (In certain states)

Even if your business isn't subject to WISP, it is best practice for risk management and data protection.

Rule Requirements

Under the WISP requirements, the framework includes:

- Risk assessment or internal and external threats.
- Multi-factor authentication (MFA) for system access.
- Encryption of sensitive data.
- Employee training on data handling and security.
- Incident response plan for breaches.
- Vendor management to ensure third-party compliance.

For tax professionals, the IRS requires confirmation of a WISP during PTIN renewal. Falsely claiming to have one can result in penalties or license revocation.

29 Bissell Street | East Hartford | CT | 06066 | www.tabinc.com
Contact our Client Success Team | 860-289-8850, option2 | clientsuccess@tabinc.com

Written Information Security Program (WISP)

Deadline

The IRS has regulated tax professionals to have the WIPS in place before renewing their PTIN, which has a deadline of December 31st each year. Firms should begin reviewing and updating their WISP well in advance to ensure compliance.

Required Information Security Elements

The WISP has ten key elements to protect data. It is required under both the FTC Safeguard Rule and IRS Publication 4557.

1. Qualified Individual
    a. Same as FTC requirement; responsible for WISP implementation.
2. Risk Assessment
    a. Identify where sensitive data resides.
3. Evaluate threats and vulnerabilities.
    a. Safeguards Implementation
4. Based on risk assessment.
    a. Includes encryption, access controls, secure disposal.
5. Monitoring and Testing
    a. Regular system scans and penetration testing.
6. Employee Training
    a. Security awareness and phishing prevention.
7. Service Provider Management
    a. Ensure vendors follow equivalent security practices.
8. Program Maintenance
    a. Update WISP as business or threat landscape changes.
9. Incident Response Plan
    a. Documented procedures for breach response.
10. Annual Review
    a. Report to leadership on WISP effectiveness and updates.
11. Compliance Mapping
    a. Align with FTC, GLBA, IRS, and state-specific laws.

TAB Compliance Manager

Our Compliance Manager has everything you need to meet the FTC Safeguard Rule. With our Compliance Manager you can simplify the compliance process, while working with an experienced IT partner.

Our Compliance Manager works in all phases of the compliance journey, from the beginning to the maintenance phase. Keeping you on track with pre-loaded policies, controls, and evidence lists available at the click of a button. Let us help you streamline and scale your compliance program.

---

https://www.rightworks.com/blog/what-is-a-wisp/
https://www.jdsupra.com/legalnews/who-needs-a-wisp-and-why-2734217/
https://www.accountingtoday.com/opinion/its-time-to-get-your-wisp-in-order
https://cybertechconnection.com/wisp/

29 Bissell Street | East Hartford | CT | 06066 | www.tabinc.com
Contact our Client Success Team | 860-289-8850, option2 | clientsuccess@tabinc.com

Written Information Security Program (WISP)

CHECKLIST

- [ ] Appoint a Qualified Individual responsible for WISP implementation.
- [ ] Conduct a risk assessment to identify sensitive data and vulnerabilities.
- [ ] Implement safeguards based on risk assessment (e.g., encryption, access controls).
- [ ] Monitor and test systems regularly for security effectiveness.
- [ ] Train employees on security awareness and phishing prevention.
- [ ] Manage service providers to ensure equivalent security practices.
- [ ] Update WISP as business operations or threats evolve.
- [ ] Maintain a documented incident response plan.
- [ ] Review WISP annually and report to leadership.
- [ ] Map WISP to applicable regulations (FTC, GLBA, IRS, state laws).

29 Bissell Street | East Hartford | CT | 06066 | www.tabinc.com
Contact our Client Success Team | 860-289-8850, option2 | clientsuccess@tabinc.com