Blue Light IT
Cyber Resilience Experts

Written Information Security Program

Written Information Security Program (WISP)

Here's a simple, Written Information Security Program (WISP) template for small CPA firms with fewer than 500 PII (Personally Identifiable Information) records. It is written to comply with the FTC Safeguards Rule and includes key elements, practical steps, and a focus on ease of implementation.
If you have more than 500 PII records, you can contact us for a customized WISP, info@bluelightit.com

Disclaimer

This Written Information Security Program (WISP) template is provided by Blue Light IT (BLIT) as a general guideline to help small CPA firms comply with the FTC Safeguards Rule. However, this template is intended for informational purposes only and should not be considered legal, regulatory, or cybersecurity advice.
Each business has unique needs, risks, and operational setups that require a customized WISP tailored to their specific circumstances. Blue Light IT (BLIT) assumes no responsibility for the accuracy, completeness, or suitability of this template for any particular business or compliance requirement.
By using this template, you acknowledge that it is your sole responsibility to adapt and implement it in alignment with your business processes, risks, and applicable regulations. For personalized assistance or to ensure compliance, consult a qualified cybersecurity or legal professional.

Written Information Security Program (WISP)

For: [Your Firm Name]
Effective Date: [Date]

1. Purpose

This WISP outlines measures to safeguard client information in compliance with the FTC Safeguards Rule. Our goal is to protect against unauthorized access, disclosure, or use of sensitive personal information.

2. Scope

This program applies to all employees, contractors, and/or third-party service providers of [Your Firm Name] who handle or have access to non-public personal information (NPI).

3. Key Definitions

- **Non-Public Personal Information (NPI):** Information obtained from a client that is not publicly available, such as Social Security numbers, financial data, and tax records.
- **PII Records:** Records containing NPI, currently under 500 within our firm.

4. Information Security Coordinator

[Name and Title] is designated as the Information Security Coordinator (ISC). Responsibilities include overseeing the implementation, maintenance, and enforcement of this WISP.

5. Risk Assessment

The ISC will conduct a risk assessment at least annually to:

1. Identify internal and external risks to client information.
2. Evaluate the effectiveness of current safeguards.
3. Update safeguards as necessary.

6. Employee Training and Management

Employees will:

- Receive training on this WISP within 30 days of hire and annually thereafter.
- Be instructed on recognizing phishing attempts, securely handling PII, and reporting incidents.

7. Safeguards

A. Physical Security

- Maintain locked file cabinets for paper records containing PII.
- Restrict access to the office after hours.

B. Technical Security

- Ensure all devices accessing client data are encrypted.
- Use strong, unique passwords for all systems, updated quarterly.
- Enable two-factor authentication (2FA) on all accounts with client data access.

- Regularly update software and antivirus programs.

C. Administrative Security

- Limit access to PII to employees who need it for their job functions.
- Require third-party vendors to sign confidentiality agreements and follow data security standards.

8. Incident Response Plan

In the event of a data breach:

1. **Contain the Breach:** Disconnect affected systems and devices.
2. **Assess the Impact:** Determine the scope and affected data.
3. **Notify Affected Parties:** Inform clients promptly if their information is compromised.
4. **Report the Incident:** Comply with regulatory reporting requirements.
5. **Evaluate and Revise:** Update safeguards to prevent recurrence.

9. Service Provider Oversight

All service providers handling PII must:

- Sign agreements confirming adherence to our data security standards.
- Provide evidence of their own information security measures upon request.

10. Annual Review and Updates

The ISC will review this WISP annually to address changes in operations, risks, or regulations. Updates will be documented and distributed to employees.

11. Record Retention and Disposal

- Retain client records only as required for business or regulatory purposes.
- Shred physical records and use secure data deletion methods for digital files when no longer needed.

12. Approval and Acknowledgment

This WISP has been reviewed and approved by [Owner/Manager Name]. All employees must read and acknowledge understanding of this program.

Approved By:

[Name, Title, Signature]

[Date]