McIntyre Financial

Written Information Security Plan (WISP)

For Tax Preparation Services

2025

Written Information Security Plan (WISP)

For Tax Preparation Services

McIntyre Financial:

Effective Date: 1/13/2025

Purpose

The purpose of this Written Information Security Plan (WISP) is to establish safeguards to protect the confidentiality, integrity, and availability of personal and financial information provided by clients for tax preparation and related services.

Scope

This plan applies to all employees, contractors, and third-party service providers of McIntyre Financial who handle, process, or store client information. It encompasses all paper and electronic records.

1. Information Security Policy

McIntyre Financial is committed to maintaining robust security practices to ensure client data is protected from unauthorized access, disclosure, alteration, or destruction.

2. Risk Assessment

We regularly assess risks to sensitive client data, including:

- Unauthorized access to or disclosure of tax documents.
- Data breaches due to malware, phishing, or other cyber threats.
- Improper disposal of physical or electronic records.

3. Data Collection and Usage

We only collect information necessary for tax preparation and compliance purposes, including but not limited to:

- Social Security Numbers (SSNs)
- Taxpayer Identification Numbers (TINs)
- Financial account details
- Employment and income records

Client data is used exclusively for authorized purposes and never shared without explicit consent, except as required by law.

4. Safeguards

Administrative Safeguards

- All employees are trained annually on data security policies and procedures.
- Access to client data is restricted to authorized personnel only.
- A designated Information Security Coordinator oversees compliance.

Technical Safeguards

- Client data is securely stored using the **software we use to file returns**, ensuring full integration and security within the tax preparation process.
- For additional storage, we use **Internxt**, a GDPR-compliant, encrypted cloud storage solution with built-in two-factor authentication (2FA).
- All data is encrypted during transmission and at rest to protect sensitive client information.
- Strong password protocols and multi-factor authentication (MFA) are enforced for all systems.
- Firewalls, antivirus software, and intrusion detection systems are maintained.

Physical Safeguards

- Paper records are stored in locked filing cabinets in secure offices.
- Shredding or secure disposal is mandatory for all discarded documents containing sensitive information.
- Workstations are locked when unattended.

5. Data Breach Response Plan

In the event of a data breach:

1. The Information Security Coordinator will be notified immediately.
2. Affected clients will be informed within 30 days of the discovery.
3. Steps will be taken to contain the breach, assess damage, and prevent recurrence.

6. Retention and Disposal

- Client records are retained for a period consistent with legal and business requirements.
- Physical documents are shredded, and electronic data is securely deleted when no longer needed.

7. Compliance with Laws and Regulations

This WISP adheres to applicable federal and state laws, including:

- IRS Publication 4557: Safeguarding Taxpayer Data
- Federal Trade Commission (FTC) Safeguards Rule
- Gramm-Leach-Bliley Act (GLBA)
- General Data Protection Regulation (GDPR)

8. Plan Review and Updates

This WISP is reviewed annually and updated as needed to address emerging risks, changes in technology, and evolving regulations.

Acknowledgment

By signing below, I acknowledge that I have read and understand the terms of the Written

Name: _____
Signature: _____
Date: _____

Approved By Board Of Directors 1/13/2025