WRITTEN INFORMATION SECURITY PLAN (WISP)

Tim Hunter CPA

TIM HUNTER CPA timhuntercpa.com 229-759-1040

Written Information Security Plan (WISP)

1. Purpose and Scope

This Written Information Security Plan (WISP) establishes the administrative, technical, and physical safeguards implemented by **Tim Hunter CPA** ("the Firm") to protect the confidentiality, integrity, and availability of taxpayer information and other sensitive data. This plan is designed to comply with:

- The Federal Trade Commission (FTC) Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA)
- Internal Revenue Service (IRS) requirements and guidance for tax professionals

This WISP applies to all partners, owners, employees, temporary staff, contractors, and third-party service providers who may access, process, store, or transmit sensitive information on behalf of the Firm.

---

2. Definitions

- **Sensitive Information**: Taxpayer data, including but not limited to Social Security numbers, EINs, dates of birth, financial account information, tax returns, payroll data, and authentication credentials.
- **Information Systems**: Any electronic or physical systems used to collect, process, store, or transmit sensitive information.
- **Authorized User**: An individual granted access to sensitive information based on job responsibilities and approval by management.

---

3. Risk Assessment

The Firm conducts an initial and ongoing risk assessment to identify reasonably foreseeable internal and external risks to sensitive information. This includes evaluating:

- Employee access levels and turnover
- Phishing, malware, ransomware, and social engineering threats
- Hardware and software vulnerabilities
- Remote access and mobile device usage
- Third-party service providers and cloud platforms
- Physical security risks (theft, fire, natural disasters)

The results of risk assessments are used to design and update safeguards outlined in this WISP.

4. Employee Management and Training

4.1 Access Controls

- Access to sensitive information is granted strictly on a **least-privilege** basis.
- Each user is assigned a unique user ID; shared logins are prohibited.
- Access rights are reviewed at least annually and immediately upon termination or role change.

4.2 Hiring and Background Practices

- Reasonable steps are taken to verify the identity and qualifications of employees prior to hiring.
- Employees are informed of their responsibility to safeguard client information.

4.3 Security Awareness Training

- All employees receive security awareness training upon hire and at least annually thereafter.
- Training includes:
    - Recognizing phishing and scam emails
    - Safe handling of taxpayer data
    - Password hygiene and MFA usage
    - Reporting suspicious activity

4.4 Confidentiality Agreements

- Employees and contractors must sign confidentiality agreements acknowledging their obligation to protect sensitive information.

---

5. Information Systems and Technical Safeguards

5.1 Authentication and Access Security

- Multi-Factor Authentication (MFA) is required for:
    - Tax preparation software
    - Remote access (VPN, cloud systems)
    - Email and cloud storage platforms
- Strong password standards are enforced (length, complexity, and periodic changes where applicable).

5.2 Network and Endpoint Security

- Firm devices are protected with:

    - Commercial-grade antivirus/anti-malware software
    - Firewalls (hardware and/or software)
    - Automatic security updates and patching
- Personal devices may only be used if approved and secured under Firm policies.

5.3 Data Encryption

- Full-disk encryption is enabled on all Firm-owned computers and laptops.
- Sensitive data transmitted electronically is encrypted using secure protocols.

5.4 Backup and Data Retention

- Encrypted backups are performed regularly and stored securely.
- Backup restoration procedures are tested periodically.
- Data is retained only as long as required by law or business necessity and securely destroyed when no longer needed.

5.5 Email and Web Security

- Spam and phishing filtering is enabled on all Firm email accounts.
- Employees are prohibited from transmitting sensitive data via unencrypted email.

---

6. Physical Safeguards

- Paper records containing sensitive information are stored in locked cabinets or offices.
- Office access is restricted to authorized personnel.
- Visitors are supervised when present in non-public areas.
- Paper documents are destroyed using cross-cut shredding or certified document destruction services.

---

7. Managing Service Providers

- The Firm evaluates third-party service providers (e.g., cloud storage, tax software, IT vendors) for their ability to safeguard sensitive information.
- Contracts require service providers to maintain appropriate security measures and notify the Firm of any data breaches.

---

8. Detecting, Responding to, and Managing Security Incidents

8.1 Incident Identification

A security incident may include:

- Malware or ransomware infection
- Unauthorized access or disclosure of data
- Lost or stolen devices
- Phishing-related credential compromise

Employees must immediately report suspected incidents to the Firm's designated Security Coordinator.

8.2 Incident Response Plan

Upon discovery of a security incident, the Firm will:

1. Contain the incident (disconnect affected systems, disable compromised accounts)
2. Preserve evidence and document findings
3. Assess the scope and impact of the incident
4. Remediate vulnerabilities
5. Restore systems from clean backups if necessary

8.3 Notification and Reporting

- The Firm will comply with all applicable federal and state breach notification laws.
- If taxpayer data is compromised, the Firm will:
    - Contact its local IRS Stakeholder Liaison
    - Follow guidance in IRS Publication 4557
    - Cooperate with law enforcement if required

---

9. Business Continuity and Disaster Recovery

- The Firm maintains procedures to ensure continued operations in the event of:
    - System failure
    - Natural disasters
    - Cyber incidents
- Critical systems and data are prioritized for recovery.

---

10. Plan Oversight and Responsibility

The Firm designates a **Security Coordinator** responsible for:

Security Coordinator: Tim L Hunter, Managing Partner

- Implementing and enforcing this WISP
- Coordinating risk assessments

- Overseeing incident response
- Ensuring employee training compliance

---

11. Monitoring, Review, and Updates

- This WISP is reviewed at least annually and whenever there are:
    - Material changes in business operations
    - New or evolving cybersecurity threats
    - Changes in IRS or FTC requirements

Updates are documented and communicated to all relevant personnel.

---

12. Related IRS Guidance and Resources

This WISP is informed by the following IRS publications:

- IRS Publication 5708 – Creating a Written Information Security Plan for Your Tax & Accounting Practice
- IRS Publication 5709 – How to Create a Written Information Security Plan for Data Safety
- IRS Publication 4557 – Safeguarding Taxpayer Data

Questions or concerns should be addressed to **contact@timhuntercpa.com**.

---

13. Approval

This Written Information Security Plan is approved and adopted by Firm management and is effective as of:

Effective Date: 2026-01-01

Approved By: Tim L. Hunter

Title: Managing Partner

Signature: