Written Information Security Plan (WISP)

Prepared for: [Your Firm Name]

Prepared under: FTC Safeguards Rule & IRS Guidance

1. Purpose & Scope

This Written Information Security Plan (WISP) establishes the administrative, technical, and physical safeguards [Your Firm Name] has implemented to protect Nonpublic Personal Information (NPI), including client, employee, and firm data.

The scope of this plan covers:

- All employees, contractors, and vendors who access or manage client information.
- All physical and electronic systems where NPI is created, stored, transmitted, or disposed of.
- All business processes involving the use of sensitive client data, including tax preparation, bookkeeping, payroll, and financial consulting.

2. Firm Profile

Firm Name: [Your Firm Name]
Number of Employees: [#]
Primary Location: [Address]
Services Offered: [Tax preparation, accounting, consulting, etc.]

3. Data Classification Policy

To ensure proper handling of information, all firm data is classified into categories:

- Public Information – Data intended for public distribution (marketing materials, website content). No restrictions apply.
- Internal Use Only – Business records not intended for external release (internal memos, training guides). Must remain within the firm.
- Confidential / NPI – Client tax returns, Social Security Numbers, financial accounts, or any information protected by federal/state law. This data requires encryption, access restrictions, and secure disposal.

Employees are responsible for knowing the classification of data they handle and following the required safeguards.

4. Risk Assessment

Risk assessments are performed annually and after major system or business changes. Each assessment includes:

- Threat Identification – Insider threats, external hackers, phishing campaigns, ransomware, lost/stolen devices, and natural disasters.

- Likelihood & Impact – Evaluation of how probable and damaging each risk is to the confidentiality, integrity, and availability of NPI.
- Safeguard Review – Assessment of current controls, such as MFA, encryption, and employee training.
- Mitigation Planning – Documenting improvements such as new controls, enhanced monitoring, or additional staff training.

Results are reviewed by the Data Security Coordinator and integrated into security updates.

5. Safeguards

Administrative Safeguards:

- Security policies are communicated to all staff and acknowledged in writing.
- Employee background checks are conducted before granting access to sensitive systems.
- Access rights are tied to job responsibilities and reviewed quarterly.

Technical Safeguards:

- Systems must run current operating systems with regular patching.
- Multi-Factor Authentication (MFA) is required for cloud services, email, and remote access.
- Encrypted backups are maintained daily and tested quarterly for restorability.
- Antivirus and endpoint detection tools are required on all firm devices.

Physical Safeguards:

- Offices secured by keyed or electronic access.
- Paper files locked in restricted areas after hours.
- Portable media (USB, CDs, external drives) not permitted without encryption and written approval.
- Visitors must sign in, be escorted, and wear identification when in restricted areas.

6. Access Control Policy

- Access is provisioned only after written authorization from management.
- User privileges are tied to job duties ("least privilege" principle).
- Access reviews are conducted quarterly to ensure only active employees have access.
- Immediately upon termination, IT disables system logins, email accounts, and remote access.
- Password Policy:
    - Minimum 12 characters with uppercase, lowercase, number, and symbol.
    - Changed every 90 days.

- Prohibited from reuse across systems.

7. Device & Mobile Security

- All firm-issued devices must be encrypted with AES-256 full-disk encryption.
- Auto-lock screens enabled after 10 minutes of inactivity.
- Mobile Device Management (MDM) allows the firm to remotely wipe or lock devices.
- Employees may not install unauthorized applications that interact with client data.
- Lost or stolen devices must be reported within 24 hours.

8. Remote Work Policy

- Only approved and secured devices may be used for remote access.
- Remote access must occur via firm-controlled VPNs or portals with MFA.
- Employees must work from a private, secure environment where screens cannot be observed by unauthorized persons.
- Paper documents used remotely must be secured in locked containers and shredded when no longer required.
- The firm reserves the right to suspend remote access in cases of non-compliance.

9. Logging & Monitoring

- System event logs capture login attempts, file access, administrative changes, and security alerts.
- Logs are stored securely for 12 months minimum.
- Quarterly reviews are performed by IT to detect unauthorized access or suspicious activity.
- Automated alerts are configured to notify administrators of repeated failed login attempts, unusual data transfers, or malware detections.

10. Vendor & Third-Party Management

- Vendors must sign confidentiality agreements and demonstrate compliance with security standards (FTC Safeguards Rule, IRS guidelines).
- Vendors with access to NPI are reviewed annually or after a significant incident.
- The firm maintains a vendor inventory documenting security contact information, services provided, and compliance certifications.
- If a vendor experiences a breach, they must notify the firm within 24 hours of discovery.

11. Incident Response Plan

In the event of a breach, suspected compromise, or system outage:

1. Containment – Immediately isolate affected systems to prevent further exposure.
2. Investigation – Identify scope, data impacted, and method of attack. Preserve logs and evidence.
3. Notification –
    a. Affected clients notified within 72 hours.
    b. Regulators and state authorities notified within statutory deadlines.
4. Remediation – Remove malware, patch vulnerabilities, reset credentials.
5. Recovery – Restore from backups if needed.
6. Documentation – Prepare a full incident report, including lessons learned.

12. Data Retention & Disposal

- Retention – Client records kept at least 7 years unless longer retention required.
- Disposal –
    - Paper: Cross-cut shredding or bonded shredding vendor.
    - Digital: Secure deletion software or device wipe protocols.
- Backups – Periodically reviewed and disposed of securely when past retention schedule.

13. Training & Awareness

- All employees trained at hire and annually thereafter.
- Training covers phishing prevention, device handling, and incident reporting.
- Employees sign an acknowledgment of WISP compliance.

14. Business Continuity & Disaster Recovery

- Daily backups stored off-site and tested quarterly.
- In case of extended outage, essential operations will continue from alternate locations or via remote systems.
- Paper fallback procedures may be used until systems are restored.
- Annual disaster recovery test performed to validate readiness.

15. Encryption & Secure Communications

- AES-256 encryption for stored data (when supported).
- TLS 1.2 or higher for web traffic and client portals.
- Password-protected PDFs with out-of-band password delivery for email attachments.

16. Program Maintenance & Review

- The WISP is reviewed annually by the Data Security Coordinator.
- Changes in technology, regulation, or business structure trigger immediate updates.
- Employee acknowledgments are re-collected with each major revision.

17. Employee Acknowledgment

I acknowledge that I have received, read, and understand the WISP for [Your Firm Name]. I agree to comply with all described policies and procedures.

Employee Name: _____ Signature: _____ Date: _____

18. Contacts for Data Security Incidents

Data Security Coordinator: [Name, Phone, Email]
IT Provider: [Vendor Name, Contact Info]

Employee Acknowledgment Log

Employee Name	Signature	Date Signed

Breach Incident Log Template

Date of Incident	Description of Breach	Systems/Clients Affected	Actions Taken	Regulatory Notifications	Resolution Date