WRITTEN INFORMATION SECURITY PLAN (WISP)

ERO Template — Compliant with IRS Pub. 4557, IRS Pub. 5708, FTC Safeguards Rule (16 CFR Part 314)

Provided by BCS Tax Software Company, LLC | For Use by Independent EROs

1. Business Information

Business / ERO Name: _____

EFIN Number: _____

PTIN Number(s): _____

Business Address: _____

Phone: _____

Email: _____

Effective Date of This WISP: _____

Next Review Date (annual): _____

2. Designated Information Security Coordinator (Qualified Individual)

Per the FTC Safeguards Rule, the ERO must designate a Qualified Individual responsible for overseeing, implementing, and enforcing this Information Security Program.

Name: _____

Title / Role: _____

Direct Phone: _____

Email: _____

3. Risk Assessment

The ERO has performed a written risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information. The risk assessment is updated annually and after any material change in business operations.

Identified risk categories (initial each that applies):

☐ Unauthorized electronic access (hacking, phishing, malware)

☐ Physical unauthorized access (lost/stolen device, office break-in)

☐ Insider threat (employee misuse)

☐ Third-party vendor/service-provider risk

☐ Natural disaster, fire, flood

☐ Hardware failure, data loss

Date of Last Risk Assessment: _____

4. Safeguards in Place

Administrative safeguards

☐ All personnel sign confidentiality agreement at hire

☐ Annual security awareness training (documented)

☐ Background checks for all personnel handling taxpayer data

☐ Written disciplinary policy for security policy violations

Technical safeguards

☐ Multi-Factor Authentication (MFA) for all systems handling customer info

☐ Encryption of data at rest (AES-256 or equivalent)

☐ Encryption of data in transit (TLS 1.2 or higher)

☐ Endpoint anti-malware / EDR on all devices

☐ Firewall configured at network perimeter

☐ Automatic software updates and patch management

☐ Secure backup with at least one off-site copy

Physical safeguards

☐ Locked filing cabinets for paper records

☐ Locked office with controlled key/keycard access

☐ Visitor sign-in log

☐ Cross-cut shredder for document disposal

☐ Secure disposal of electronic media (wipe / physical destruction)

5. Employee Access & Training

Access to taxpayer information is restricted to personnel with a documented business need. All personnel receive security training at onboarding and annually thereafter. Training records are retained for at least 3 years.

Date of Last Annual Training: _____

Trainer / Provider: _____

6. Vendor / Third-Party Risk Management

All third-party service providers handling taxpayer data must agree in writing to maintain security safeguards consistent with this WISP and IRS / FTC requirements.

Approved third-party service providers (list):

Vendor: _____

Vendor: _____

Vendor: _____

Vendor: _____

Vendor: _____

7. Data Retention & Disposal

Taxpayer information is retained only as long as necessary for the purpose collected and as required by law (minimum 3 years per IRS regulations). Disposal is performed by shredding for paper and certified wiping or physical destruction for electronic media.

8. Incident Response Plan

In the event of a suspected or actual breach of taxpayer information:

a. The Qualified Individual is notified immediately.

b. The breach is contained (systems isolated, accounts disabled).

c. The Company (BCS Tax Software Company, LLC) is notified in writing within 24 hours.

d. Affected taxpayers are notified per applicable state breach-notification law.

e. The IRS is notified per Pub. 4557 / Pub. 5708 guidance.

f. A post-incident review is conducted, and this WISP is updated as needed.

9. Annual Testing & Monitoring

Per the FTC Safeguards Rule, the ERO conducts at least one of the following annually:

☐ Penetration testing (external)

☐ Continuous monitoring of in-scope systems

Date / Provider of Last Test: _____

10. Annual Report to Governing Body

The Qualified Individual presents an annual written report on the state of the Information Security Program, including: (a) overall status, (b) material matters relating to security, (c) recommendations for changes.

Date of Last Annual Report: _____

11. Acknowledgment & Signature

I acknowledge that this WISP has been adopted, implemented, and is being maintained for the business identified above. I understand the IRS and FTC require ongoing compliance and that failure to maintain this WISP may result in PTIN/EFIN suspension, civil penalties, and termination of my agreement with BCS Tax Software Company, LLC.

ERO Owner Signature

_____

Printed Name: _____

Title: _____

Date: _____

Disclaimer: This template is provided as a starting point for compliance. EROs are responsible for tailoring it to their specific operations and reviewing with qualified legal/compliance counsel. BCS Tax Software Company, LLC is not a law firm and this is not legal advice.