WRITTEN INFORMATION SECURITY PLAN

# Cedar Park Tax Service LLC (SAMPLE — fictional firm)

d/b/a Cedar Park Tax (sample)

Prepared under the Gramm-Leach-Bliley Act and the FTC Safeguards Rule (16 CFR Part 314), following the outline of IRS Publication 5708.

| Item | Detail |
|---|---|
| Effective date | December 01, 2026 |
| Version | 1.0 |
| Qualified Individual / Data Security Coordinator | A. Sample, EA, Owner / Managing Member |
| Owner / principal | A. Sample, EA, Owner / Managing Member |
| Next scheduled review | December 01, 2027 (at least annually, or after any material change) |
| Distribution | All personnel. Available to clients on request with the DSC's consent. |

**Important - please read**

This plan was drafted from the firm's own answers as a starting point. It is not legal, tax, or professional advice, is not endorsed or approved by the IRS or the FTC, and does not by itself make the firm compliant with any law. The firm is responsible for reviewing, tailoring, implementing, and maintaining it, and should consult a qualified attorney or security professional as needed.

# Plan at a glance

Cedar Park Tax (sample) handles taxpayer and client information that criminals actively target. This plan describes how the firm protects it, who is responsible, and what happens if something goes wrong. Based on the firm's answers, 5 high-priority and 7 other improvement items were identified. Each one is listed below with a target date; the Data Security Coordinator tracks them to completion.

### Fewer than 5,000 consumers

Under 16 CFR 314.6, firms that maintain information on fewer than 5,000 consumers are exempt from §314.4(b)(1) (written risk assessment), §314.4(d)(2) (annual penetration test and semi-annual vulnerability assessments), §314.4(h) (written incident response plan) and §314.4(i) (annual written report). This plan still includes a risk assessment and incident response plan because IRS Publication 5708 recommends them and they are inexpensive to maintain.

## Action plan

| Priority | Item | What to do | Rule ref. | Target |
|---|---|---|---|---|
| High | MFA on remote access | Require MFA for all remote access. | 314.4(c)(5) | Dec 31, 2026 |
| High | Encryption at rest | Enable BitLocker/FileVault (or NAS volume encryption) on: Desktop workstation; Laptop. Printers/scanners: enable storage encryption or auto-erase where supported. | 314.4(c)(3) | Dec 31, 2026 |
| High | Security awareness training | Hold training before filing season and annually; collect signed acknowledgments (Attachment D). | 314.4(e)(1) | Dec 31, 2026 |
| High | Phishing & call-back verification | Train staff to verify any request for data, payments or credential changes by calling a known number. | 314.4(e)(1) | Dec 31, 2026 |
| High | Email spoofing protection (grade D) | Publish DKIM and DMARC so criminals cannot send email in the firm's name (records in Attachment H). | 314.4(c) / Pub 4557 | Dec 31, 2026 |
| Medium | Incident contacts | Complete the contact sheet in Attachment C and keep a printed copy off-site. | 314.4(h) | Dec 15, 2026 |
| Medium | Guest Wi-Fi separation | Create a separate guest network for clients and visitors. | 314.4(c)(1) | Dec 31, 2026 |
| Medium | Off-site backups | Add an encrypted, automatic off-site/cloud backup and test a restore each quarter. | 314.4(c), (d)(1) | Dec 31, 2026 |
| Medium | Password manager | Adopt a business password manager with MFA for all staff. | 314.4(c)(1) | Jan 15, 2027 |
| Medium | Activity logging | Turn on and review sign-in/audit logs (email, tax software, NAS) monthly. | 314.4(c)(8) | Jan 15, 2027 |
| Medium | Service-provider contracts | Obtain written safeguarding terms from each provider in Attachment G; keep on file. | 314.4(f)(2) | Jan 30, 2027 |
| Low | Cyber insurance | Consider a cyber/data-breach policy; insurers typically ask about MFA, backups and email authentication. | Best practice | Mar 01, 2027 |

# I. Objective

Our objective, in developing and implementing this Written Information Security Plan (WISP), is to create effective administrative, technical, and physical safeguards to protect the Personally Identifiable Information (PII) retained by Cedar Park Tax Service LLC (SAMPLE — fictional firm) ("the Firm"). This WISP is intended to comply with the Firm's obligations under the Gramm-Leach-Bliley Act and the Federal Trade Commission Financial Privacy and Safeguards Rules. It sets out how the Firm accesses, collects, stores, uses, transmits, and protects PII.

For this WISP, PII means a taxpayer's, spouse's, dependent's, or employee's first name or initial and last name combined with any of the following:

- **A.** Social Security number, ITIN, date of birth, or employment data;
- **B.** Driver's license or state ID number;
- **C.** Income, tax filing, retirement plan, asset ownership, or investment data;
- **D.** Financial account, credit or debit card numbers, PINs, or passwords that permit access to financial accounts;
- **E.** Email addresses, unlisted phone numbers, or residential contact information.

PII does not include information lawfully obtained from publicly available sources or government records made available to the general public.

# II. Purpose

- **A.** Ensure the security and confidentiality of all PII retained by the Firm.
- **B.** Protect PII against anticipated threats or hazards to its security or integrity.
- **C.** Protect against unauthorized access to or use of PII that could result in identity theft, refund fraud, or other harm.

# III. Scope

This WISP applies to all owners, employees, seasonal staff, and contractors of the Firm, to all locations (Main office (commercial office): [Street address redacted], Windermere, FL 34786; Seasonal annex (shared / coworking): [Street address redacted], Winter Garden, FL), and to all paper and electronic records containing PII, wherever stored, including cloud services and personal devices used for Firm work. The Firm provides: individual tax returns (1040), business returns (1120, 1120-s, 1065), bookkeeping / payroll, irs representation.

- **A.** Identify reasonably foreseeable internal and external risks to records containing PII.
- **B.** Assess the likelihood and potential damage of these threats, considering the sensitivity of the PII.
- **C.** Evaluate the sufficiency of existing policies, procedures, systems, and safeguards.
- **D.** Design and implement safeguards to minimize those risks, consistent with the Safeguards Rule and NIST recommendations.
- **E.** Regularly monitor and assess the effectiveness of those safeguards.

# IV. Identified responsible officials

The Firm designates A. Sample, EA (Owner / Managing Member) as the Qualified Individual and Data Security Coordinator (DSC) under 16 CFR 314.4(a). The DSC implements, supervises, and maintains this WISP and is responsible for:

- Implementing the WISP, including daily operational protocols;
- Identifying all repositories of PII and designating them as Secured Assets with Restricted Access;
- Verifying that all personnel complete security training before access and annually thereafter;
- Monitoring and testing compliance with this plan;
- Selecting, contracting with, and periodically assessing service providers that access PII (Attachment G);
- Reviewing this WISP at least annually and whenever there is a material change in the business;
- Reporting in writing at least annually to the owner on the status of the program, risks, incidents, and recommended changes.

The Firm designates B. Sample as Public Information Officer (PIO). All outward communication after a security incident (clients, law enforcement, media, business partners) is approved by the PIO in consultation with the DSC.

## Authorized users and access levels

| Name | Role | Type | Access level |
|---|---|---|---|
| A. Sample, EA | Owner, preparer | Owner | Full |
| B. Sample | Office manager | W-2 | Full |
| C. Sample, CPA | Seasonal preparer | Seasonal W-2 | Tax software and client files only |

# Risk assessment

The Firm assesses risks by likelihood (Low/Medium/High) and impact on the confidentiality, integrity, and availability of client information. Risks rated High are treated first; Medium risks are reduced within the action plan; Low risks may be accepted by the DSC in writing. The assessment is repeated at least annually and after any incident or major change.

| Risk | Likelihood | Impact | Current safeguards | Treatment |
|---|---|---|---|---|
| Phishing / credential theft of email or tax software | High | High | MFA on email; MFA on tax software | MFA everywhere; annual phishing training; call-back verification |
| Impersonation of the Firm by email (spoofing) | High | Medium | Email check grade D | Publish DKIM and enforce DMARC (Attachment H) |
| Ransomware / malware | Medium | High | anti-malware; auto updates; Automatic, local only | Patching, anti-malware, encrypted off-site backups with tested restores |
| Lost or stolen laptop/ phone | Medium | High | None reported | Full-disk encryption on all devices; remote wipe for phones |

| Risk | Likelihood | Impact | Current safeguards | Treatment |
|---|---|---|---|---|
| Unauthorized physical access to paper files | Low | High | locked storage; shredding | Locked cabinets, clean desk, visitor escort |
| Insider misuse or excess access (incl. seasonal staff) | Low | High | unique accounts | Least privilege; remove access at season end; review logs monthly |
| Service provider breach | Medium | High | None reported | Vendor due diligence and contract terms (Attachment G) |
| Remote access compromise | Medium | High | None reported | MFA on all remote tools; disable unused remote access |

Information the Firm handles: taxpayer identity data (SSN/ITIN, DOB, IDs), income and tax documents, bank account and refund data.

Monitoring and testing: the DSC reviews sign-in alerts and security software reports monthly, checks backups by performing a test restore quarterly, reviews user access before and after each filing season, and arranges a vulnerability review of internet-facing systems at least annually.

# V. Inside-the-firm risk mitigation

## PII collection and retention policy

**A.** The Firm collects only the PII needed for legitimate business purposes and legal obligations.

**B.** Access to PII is limited to personnel whose duties require it (see Authorized users).

**C.** PII is stored only in these approved locations: Local file server / NAS, Encrypted USB drives; tax software (Drake Tax); client portal (None). Any new storage location requires DSC approval.

**D.** Records are retained for 7 years after the last use unless a longer period is required by law, then securely destroyed. The DSC documents the business or legal reason for this period and reviews it annually, consistent with 16 CFR 314.4(c)(6), which calls for disposal no later than two years after last use unless retention is necessary for business or legal reasons (see Attachment A).

**E.** Paper is destroyed by cross-cut shredding or a certified shredding service; electronic media is wiped or physically destroyed before disposal or return.

## Personnel accountability policy

**A.** Every person receives this WISP at onboarding and signs the acknowledgment (Attachment D) before receiving access, and again after annual training.

**B.** Personnel follow the Rules of Behavior (Attachment B) and report any suspected incident to the DSC immediately.

**C.** Violations may result in discipline up to termination and, where applicable, legal action.

**D.** Access is removed on the day a person leaves the Firm or a seasonal engagement ends; shared credentials they knew are changed.

### PII disclosure policy

**A.** PII is not disclosed without verifying the identity of the recipient and having the client's authorization, except as required by law.

**B.** Requests to change bank account, refund, or contact details, or to send records, are verified by calling the client at a phone number already on file - never one provided in the request.

**C.** Employee PII is shared only with payroll, benefits, and insurance providers bound by written confidentiality terms.

### Reportable event policy

Any suspected data security incident is handled under the Security Breach Procedures in Attachment C. The DSC maintains any cyber insurance and coordinates notifications to the IRS Stakeholder Liaison, state agencies, affected individuals, and the FTC where required.

## VI. Outside-the-firm risk mitigation

### Network protection policy

**A.** Firewalls are enabled on the internet router and on every computer.

**B.** Operating systems and software are updated automatically; the DSC verifies monthly that no device is out of date.

**C.** All computers run current, licensed anti-malware software with real-time protection.

**D.** Unsupported (end-of-life) operating systems and routers are not used for Firm work.

**E.** Router administrative passwords are changed from defaults and remote router administration is disabled.

### User access control policy

**A.** Multi-factor authentication (MFA) is required for any individual accessing any information system containing PII, including email (Microsoft 365), tax software, IRS e-Services, the client portal, cloud storage, and remote access, as required by 16 CFR 314.4(c)(5). Any exception must be approved in writing by the DSC with an equivalent control.

**B.** Every user has a unique account. Shared accounts and shared passwords are prohibited.

**C.** Passwords follow current NIST SP 800-63B guidance: long passphrases (at least 14 characters recommended), no reuse, and changes when compromise is suspected. The Firm will adopt a business password manager (see action plan).

**D.** Administrative rights on computers are limited to the DSC and the IT provider.

### Electronic exchange of PII policy

**A.** PII is never sent as an unprotected email attachment. Files are exchanged through the client portal (None) or encrypted email; passwords are shared by a separate channel.

**B.** Removable media containing PII is encrypted (e.g., BitLocker To Go) and inventoried.

**C.** Email authentication (SPF, DKIM, DMARC) is maintained on the Firm's domain to reduce spoofing of the

Firm's name (see Attachment H).

### Wi-Fi access policy

**A.** Firm Wi-Fi uses WPA2 encryption with a strong passphrase known only to authorized personnel.

**B.** Clients and visitors use a separate guest network that cannot reach Firm devices. (To be implemented - see action plan.)

**C.** Public Wi-Fi is not used for Firm work unless connected through the Firm-approved VPN.

### Remote access policy

**A.** Approved remote access method: Remote desktop tool (e.g., TeamViewer/SplashTop) without MFA. Remote access requires MFA and is limited to authorized users.

**B.** Remote sessions are not left unattended; devices lock automatically after 10 minutes of inactivity.

**C.** Home offices follow the same physical and technical safeguards as the main office.

### Connected devices policy

**A.** New devices are reviewed and configured by the DSC or IT provider before connecting to the Firm network.

**B.** AutoRun for USB and optical media is disabled.

**C.** Copiers, scanners, and computers are wiped or their drives destroyed before disposal, return, or resale.

**D.** Mobile phones used for Firm email or MFA use a screen lock, encryption, and automatic updates.

### Information security training policy

All personnel complete security awareness training before receiving access and at least annually before filing season. Training covers phishing and impersonation, call-back verification, safe handling of PII, password and MFA use, and how to report incidents. Attendance is documented on Attachment D. The DSC keeps current on threats through IRS and Security Summit alerts (e.g., IRS Publication 4557 and e-News for Tax Professionals).

### Service provider oversight

The Firm selects providers capable of safeguarding customer information, requires safeguards by contract, and reassesses them at least annually (16 CFR 314.4(f)). Providers are listed in Attachment G.

## VII. Implementation

Effective December 01, 2026, Cedar Park Tax Service LLC (SAMPLE — fictional firm) adopts this Written Information Security Plan in compliance with the Gramm-Leach-Bliley Act and the FTC Financial Privacy and Safeguards Rules. The plan will be reviewed at least annually and after any material change or security event.

Signed: _____ Date: _____

A. Sample, EA - Owner / Managing Member

Signed: _____ Date: _____

A. Sample, EA - Data Security Coordinator / Qualified Individual

## Attachment A: Record retention and disposal

| Record type | Retention | Disposal method |
|---|---|---|
| Client tax returns and workpapers | 7 years after filing (documented business/ legal reason) | Cross-cut shred / secure delete |
| Client source documents (W-2, 1099, IDs) | Return originals to client; scanned copies per above | Shred paper copies after scanning |
| Forms 8879 (e-file signature) | 3 years from the return due date or IRS receipt, whichever is later (per IRS e-file rules) | Secure delete / shred |
| Payroll and employee records | As required by law (generally 4+ years) | Cross-cut shred / secure delete |
| Prospective-client data (no engagement) | Delete within 90 days | Secure delete |
| Old computers, drives, copiers | Until replaced | Certified wipe or physical destruction; keep certificate |

*The DSC reviews this schedule annually; confirm periods with your professional advisor and applicable state rules.*

## Attachment B: Rules of behavior for safeguarding client PII

- Lock your screen whenever you step away; never share your password or MFA codes.
- Never send PII by regular email, text, or messaging apps; use the client portal.
- Verify any request to change bank details, addresses or to send files by calling the client at the number on file.
- Do not install software, browser extensions, or connect USB devices without DSC approval.
- Do not use personal email or personal cloud storage for Firm data.
- Keep paper with PII in locked storage; shred, never trash.
- Do not discuss client information in public places or on social media.
- Report lost devices, suspicious emails, or unusual account activity to the DSC immediately - speed matters more than certainty.

## Attachment C: Security incident procedures and contacts

If an incident is suspected: (1) do not turn off affected computers - disconnect them from the network; (2) notify the DSC immediately; (3) the DSC leads containment, preserves evidence, and coordinates the steps below; (4) document every action with date and time.

| Who | When | How / notes |
|---|---|---|
| Data Security Coordinator | Immediately | A. Sample, EA - phone: _____ |
| IT provider | Immediately | Owner, with an on-call vendor - phone: _____ |
| IRS Stakeholder Liaison | As soon as data theft is suspected | irs.gov/stakeholder-liaison (find the liaison for the Firm's state) |

| Who | When | How / notes |
|---|---|---|
| Florida Department of Revenue | Per state guidance | Federation of Tax Administrators: taxadmin.org (state alert contacts) |
| Local police / FBI IC3 | If a crime occurred | Local police report; ic3.gov |
| Cyber insurance carrier | Per policy (often within 24-72 h) | Policy # _____ |
| Affected individuals and state officials | Per state law (summary below) | Fla. Stat. § 501.171 |
| Federal Trade Commission | No later than 30 days after discovery if 500+ consumers' unencrypted information was acquired without authorization | FTC online Safeguards Rule notification form (16 CFR 314.4(j)) |
| EFIN / e-Services account | If e-file credentials may be compromised | Contact the IRS e-help Desk; review e-Services account and accepted-returns counts |

## State breach-notification summary: Florida

**Fla. Stat. § 501.171.** Notify affected Florida residents by mail or email as expeditiously as practicable and no later than 30 days after determining the breach (law-enforcement delay or a documented no-harm determination may apply; the determination must be kept 5 years and sent to the Department within 30 days). If 500 or more Floridians are affected, notify the Department of Legal Affairs (Attorney General) within 30 days (15 more days for good cause). If more than 1,000 people are notified at once, notify the nationwide consumer reporting agencies. Vendors (third-party agents) must tell the firm within 10 days. Records containing personal information must be securely disposed of. Failure to notify can cost up to $500,000 per breach. Personal information now includes biometric and geolocation data (ch. 2026-52).

*Source: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/Sections/0501.171.html (verified 2026-11-18). Summary for planning only; confirm with counsel at the time of an incident.*

Clients who live in other states may trigger those states' laws as well; the DSC checks each affected state's rules during an incident.

After the incident, the DSC documents root cause and remediation, and updates this WISP and the risk assessment (16 CFR 314.4(h)(5)-(7)).

## Attachment D: Employee/contractor acknowledgment of understanding

I have received, read, and understand the Written Information Security Plan of Cedar Park Tax Service LLC (SAMPLE — fictional firm). I agree to follow its policies and the Rules of Behavior, to complete required training, and to report suspected incidents immediately. I understand that violations may result in disciplinary action up to termination.

| Name | Role | Training date | Signature | Date |
|---|---|---|---|---|
| A. Sample, EA | Owner, preparer | | | |
| B. Sample | Office manager | | | |
| C. Sample, CPA | Seasonal preparer | | | |
| | | | | |
| | | | | |
| | | | | |

## Attachment E: Hardware inventory containing PII

| Device | Location | Primary user | PII stored/processed | Encrypted |
|---|---|---|---|---|
| Desktop workstation | Main office | A. Sample | Tax software and client files | No - action |
| Laptop | Travel / seasonal annex | C. Sample | Working copies of returns | No - action |

## Attachment F: Personnel authorized to access PII

| Name | Access level | Systems | Access granted | Access removed |
|---|---|---|---|---|
| A. Sample, EA | Full | Tax software, portal | | |
| B. Sample | Full | Tax software, portal | | |
| C. Sample, CPA | Tax software and client files only | Tax software, portal | | |

## Attachment G: Service providers with access to PII

| Provider | Service | Safeguards in contract? (Y/N, date) | Last reviewed |
|---|---|---|---|
| Drake Tax | Tax preparation software | | |
| Microsoft 365 | Email | | |
| None | Client document portal | | |
| Owner, with an on-call vendor | IT support (administrative access) | | |
| Example Payroll Co. | Payroll processing (sample) | | |
| Example Bank | Business checking (sample) | | |

# Attachment H: Email spoofing check

**Domain: example-sample.invalid  Grade: D (56/100)  [SIMULATED for this sample]**

SPF present (~all). DKIM not found on common selectors. No DMARC record. This is a simulated check for the public sample.

| Fix | Type | Host | Value |
|---|---|---|---|
| Publish a DMARC record (start with p=none, then move to reject) | TXT | _dmarc | v=DMARC1; p=none; rua=mailto:dmarc-reports@example-sample.invalid; fo=1 |
| Turn on DKIM signing at your email provider | CNAME/TXT | see provider | generated by your email provider |

*Passive check of public DNS records only. Re-check after changes and at each annual review.*

# Attachment I: FTC Safeguards Rule crosswalk

| 16 CFR 314.4 | Requirement (summary) | Where in this plan |
|---|---|---|
| (a) | Qualified Individual | Section IV |
| (b) | Written risk assessment (exempt <5,000; included) | Risk assessment |
| (c)(1) | Access controls | User access control; Authorized users |
| (c)(2) | Inventory of data, devices, systems | Attachments E, F, G |
| (c)(3) | Encryption in transit and at rest | Electronic exchange; action plan |
| (c)(4) | Secure development (in-house apps) | Not applicable - no in-house applications |
| (c)(5) | Multi-factor authentication | User access control |
| (c)(6) | Secure disposal; retention review | Retention policy; Attachment A |
| (c)(7) | Change management | Connected devices; Network protection |
| (c)(8) | Monitor and log user activity | Monitoring and testing; action plan |
| (d) | Testing / monitoring ((d)(2) exempt <5,000) | Risk assessment - monitoring and testing |
| (e) | Training and qualified personnel | Training policy; Attachment D |
| (f) | Service-provider oversight | Service provider oversight; Attachment G |
| (g) | Evaluate and adjust | Section VII; annual review |
| (h) | Incident response plan (exempt <5,000; included) | Attachment C |
| (i) | Annual written report to owner/board (exempt <5,000) | Section IV (DSC duties) |
| (j) | FTC notice, 500+ consumers, within 30 days | Attachment C |

## Review log

| Date | Reviewed by | Changes made |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**Disclaimer**

This plan was drafted from the firm's own answers as a starting point. It is not legal, tax, or professional advice, is not endorsed or approved by the IRS or the FTC, and does not by itself make the firm compliant with any law. The firm is responsible for reviewing, tailoring, implementing, and maintaining it, and should consult a qualified attorney or security professional as needed.