WRITTEN INFORMATION SECURITY PLAN

Riverside Tax & Bookkeeping LLC

1200 Main Street, Suite 4, Jacksonville, Florida

Effective date: November 15, 2026

Last reviewed: November 15, 2026

Plan owner (Qualified Individual): Marcus Hill, Office Manager

This plan is available to all personnel. Clients may request a copy with the approval of the Qualified Individual.

Prepared under the Gramm-Leach-Bliley Act and the FTC Safeguards Rule (16 CFR Part 314). Format follows IRS Publication 5708.

Contents

- 1. Objective, Purpose and Scope
- 2. Responsible Individuals
- 3. Risk Assessment
- 4. Safeguards
- 5. Testing and Monitoring
- 6. Personnel, Training and Accountability
- 7. Service Provider Oversight
- 8. Program Evaluation and Annual Report
- 9. Incident Response Plan
- 10. FTC Notification Requirement
- 11. Corrective Action Plan
- Implementation and Signatures
- Attachment A — Record Retention and Disposal Schedule
- Attachment B — Rules of Behavior for Safeguarding Client Data
- Attachment C — Incident Response Checklist
- Attachment D — Employee and Contractor Acknowledgment (Training Sign-off)
- Attachment E — Hardware and Data Inventory
- Attachment F — Personnel Authorized to Access Client Data
- Attachment G — Service Provider Register
- Attachment H — Annual Review and Qualified Individual Report Log
- Attachment I — Safeguards Rule Compliance Map

> Small-firm note: Riverside Tax & Bookkeeping LLC maintains customer information on fewer than 5,000 consumers. Under 16 CFR 314.6, four items are not legally required for firms this size: the written risk assessment (314.4(b)(1)), penetration testing and vulnerability assessments (314.4(d)(2)), the written incident response plan (314.4(h)) and the annual written report (314.4(i)). The Firm keeps all four as best practice because they are what investigators, insurers and the IRS look for after a breach.

1. Objective, Purpose and Scope

1.1 Objective

This Written Information Security Plan (WISP) sets out the administrative, technical and physical safeguards Riverside Tax & Bookkeeping LLC (the Firm) uses to protect the personally identifiable information (PII) of its clients and employees. The Firm is a financial institution under the Gramm-Leach-Bliley Act, and this plan is written to meet the Federal Trade Commission Safeguards Rule, 16 CFR Part 314.

1.2 Purpose

- Keep all PII held by the Firm secure and confidential.
- Protect PII against anticipated threats or hazards to its security or integrity.
- Prevent unauthorized access to or use of PII that could result in identity theft, fraud or other harm to clients.

1.3 What counts as PII

For this plan, PII means a person's first name or first initial and last name, combined with any of the following, for clients, client family members, business entities or Firm employees:

- Social Security number, ITIN, date of birth or employment information
- Driver's license or state ID number
- Income, tax filing, retirement, asset or investment information
- Bank account, credit or debit card numbers, and any code or password that gives access to them
- Email addresses, unlisted phone numbers and home contact details

Information lawfully available to the public, such as a published phone directory listing, is not PII under this plan.

1.4 Scope

This plan covers every record containing PII, in any format — paper, electronic, or held by a service provider — and every owner, employee, seasonal worker and contractor who can reach it. It covers the Firm's office at 1200 Main Street, Suite 4, Jacksonville, Florida, any remote work location, and all devices and cloud services used for Firm business.

2. Responsible Individuals

2.1 Qualified Individual (Data Security Coordinator)

The Firm designates Marcus Hill, Office Manager, as its Qualified Individual under 16 CFR 314.4(a). The Qualified Individual also serves as the Data Security Coordinator described in IRS Publication 5708.

Contact: marcus@riversidetax.example · (904) 555-0143

The Qualified Individual is responsible for:

- Running this plan day to day and enforcing it.
- Keeping the inventories in Attachments E, F and G current.
- Making sure every person completes security training before getting access to PII and again each year (Attachment D).
- Checking staff compliance with this plan and the rules in Attachment B.
- Selecting, contracting with and periodically assessing service providers.
- Running the incident response plan in Section 9.
- Reviewing this plan each November and whenever the Firm's operations change in a way that affects client data.
- Reporting in writing to the owner at least once a year (Section 8.2).

2.2 Public Information Officer

The Firm designates Denise Carter as Public Information Officer (PIO). During a security incident the PIO is the only person who speaks for the Firm to clients, the news media, neighboring businesses and trade associations. Statements to law enforcement are coordinated between the PIO and the Qualified Individual.

2.3 Owner

Denise Carter, Owner, Enrolled Agent, approves this plan, receives the Qualified Individual's annual report, and provides the time and budget needed to carry the plan out.

3. Risk Assessment

This written risk assessment meets 16 CFR 314.4(b). It identifies reasonably foreseeable internal and external risks to the security, confidentiality and integrity of client information and assesses whether current safeguards control them.

3.1 Information the Firm handles

- Client tax returns, source documents (W-2s, 1099s, K-1s), identity documents and prior-year returns
- Client bank account and routing numbers for refunds and payments
- Engagement letters, consent forms (including Section 7216 consents) and correspondence
- Employee personnel and payroll records
- Paper files and printouts containing PII
- Credentials for IRS e-Services, the Firm's EFIN and tax software accounts

3.2 Evaluation criteria

Each risk is scored for likelihood and impact on the confidentiality, integrity and availability of client information, using the criteria below (16 CFR 314.4(b)(1)(i)–(ii)).

Rating	Likelihood	Impact
Low	Unlikely in the next year given current controls	Little or no client data exposed; operations unaffected
Medium	Could happen in the next year	Limited exposure or a short disruption; some clients affected
High	Expected, or has happened to similar firms	Large exposure, fraudulent returns, or operations stopped

Overall rating: High if one factor is High and the other is at least Medium; Low if both are Low or one is Low and the other Medium; Medium otherwise.

How risks are treated (16 CFR 314.4(b)(1)(iii)): High risks are mitigated within 30 days. Medium risks are mitigated within 90 days or accepted in writing by the Qualified Individual with a stated reason. Low risks are accepted and monitored at the annual review.

3.3 Risk register

Risk	Likelihood	Impact	Rating	Key controls	Decision
Phishing email or text that steals passwords	H	H	High	MFA on every system; annual training; email filtering; call-back rule for unexpected requests	Mitigate
Remote access takeover of an office computer	M	H	High	MFA on the remote tool; access only during staffed hours; session logging	Mitigate
Ransomware or other malware	M	H	High	Automatic patching; anti-malware on every device; tested off-site backups	Mitigate
Lost or stolen laptop or phone	M	M	Medium	Full-disk encryption; screen lock; remote wipe where available	Mitigate
Staff misuse or access beyond job need	L	H	Medium	Least-privilege access (Attachment F); unique logins; log review; background checks	Mitigate
Theft or exposure of paper records	M	M	Medium	Locked storage; clear-desk rule; shredding service	Mitigate
Breach at a cloud or software provider	M	H	High	Vendor selection and contract terms (Attachment G); MFA on vendor accounts; annual vendor review	Mitigate
Misuse of the Firm's EFIN or e-Services account	M	H	High	Weekly check of e-file counts in IRS e-Services; MFA; restricted e-Services roles	Mitigate
Client data sent to the wrong person or in	L	M	Low	Secure portal or encrypted files; passwords sent by a separate channel;	Accept and monitor

Risk	Likelihood	Impact	Rating	Key controls	Decision
plain email				verify recipient	
Network intrusion through Wi-Fi or connected devices	L	H	Medium	Encrypted Wi-Fi; guests kept off the Firm network; default passwords changed	Mitigate
Hurricane, fire, flood or long power outage	M	H	High	Off-site encrypted backups; copy of this plan stored off site; tax software provider contact list	Mitigate

The Qualified Individual repeats this assessment at least once a year and whenever the Firm adds a system, location, service provider or type of client data (16 CFR 314.4(b)(2)).

4. Safeguards

The Firm uses the following safeguards to control the risks above (16 CFR 314.4(c)).

4.1 Access control

- Every person has a unique login. Shared accounts and shared passwords are not allowed on any system that holds client data, including tax software, email, cloud storage and IRS e-Services.
- People get access only to the client information they need for their job (least privilege). Access levels are listed in Attachment F and reviewed at least once a year.
- Access is removed the same day a person leaves the Firm or changes roles.
- Paper files are kept in locked storage (locked file room, back office) and areas holding PII are closed to visitors unless escorted.

4.2 Data and systems inventory

The Firm keeps an inventory of the devices, systems and locations that store or process client data (Attachment E) and of the people authorized to access it (Attachment F). Systems in use:

- Tax software: Drake Tax
- Other business software: QuickBooks Online, Gusto payroll
- Email: Microsoft 365
- Cloud storage: Microsoft OneDrive
- Client file exchange: secure client portal (SmartVault)

4.3 Encryption

All client information is encrypted when sent over external networks and when stored (16 CFR 314.4(c)(3)):

- In transit: websites, portals and cloud services are used only over encrypted connections (HTTPS/TLS). Client files are never sent as plain email attachments.

- At rest: Full-disk encryption (BitLocker on Windows, FileVault on Mac) is on for every computer; business phones use device encryption; only encrypted USB drives may hold PII.

4.4 Applications

The Firm does not develop its own software. Before adopting any externally developed application that stores, transmits or accesses client information, the Qualified Individual confirms that it supports multi-factor authentication, encrypts data, and comes from a vendor with a published security program (16 CFR 314.4(c)(4)).

4.5 Multi-factor authentication

Multi-factor authentication (MFA) is required for every person who accesses any information system containing client information (16 CFR 314.4(c)(5)), including tax software, email, cloud storage, the client portal, remote access tools and IRS e-Services. The Firm uses an authenticator app (for example Microsoft Authenticator, Google Authenticator or Duo). Any exception requires the Qualified Individual's written approval of a reasonably equivalent or stronger control.

4.6 Retention and secure disposal

- The Firm collects only the PII needed to prepare returns and run the business.
- Client tax records are kept for 4 years. Federal law requires preparers to keep a copy of each return, or a list of clients and returns prepared, for 3 years (IRC §6107(b)).
- Customer information is securely disposed of no later than two years after it was last used to serve the client, unless it is still needed for business operations or another legitimate business purpose, the law requires keeping it, or targeted disposal is not reasonably feasible (16 CFR 314.4(c)(6)).
- Paper is destroyed by a contracted shredding service (Bold City Shredding). Drives and devices are wiped or physically destroyed before disposal, resale or return.
- The retention schedule (Attachment A) is reviewed every November.

4.7 Change management

No new software, device, cloud service or remote access tool is connected to Firm systems until the Qualified Individual approves it. Each change is recorded with the date, what changed, who approved it and how it was tested. Security settings are rechecked after major updates (16 CFR 314.4(c)(7)).

4.8 Monitoring and logging

Activity logging stays on for every system that holds client data, including sign-in logs for Microsoft 365, audit logs in the tax software and Windows/Mac security logs. The Qualified Individual or First Coast IT Services reviews logs for unauthorized access or tampering at least every 90 days and immediately after any alert (16 CFR 314.4(c)(8)).

4.9 Network, Wi-Fi and devices

- A firewall sits between the internet and the office network, and each computer's built-in firewall is on.

- Operating systems, browsers and all software receive security updates automatically. The Qualified Individual checks update status at least every 30 days.
- Anti-malware protection runs on every computer and stays current.
- Office Wi-Fi uses WPA2 or WPA3 encryption with a strong password. Guests use a separate guest network that cannot reach Firm devices.
- Default passwords on routers, printers, copiers and other connected devices are changed before use. AutoRun is disabled for USB and optical drives.
- Passwords are at least 12 characters, unique to each system, never reused for personal accounts, and changed immediately when compromise is suspected. A password manager approved by the Qualified Individual may be used if it is encrypted and protected by MFA.
- Client PII may not be stored on personal devices, personal email or personal cloud accounts.

4.10 Remote access

Remote access is allowed only through Splashtop with MFA, with MFA and an encrypted connection, for users approved by the Qualified Individual. Remote access is limited to staffed business hours, when unusual activity will be noticed. Unattended remote access software is not installed on any computer.

4.11 Sending and sharing client information

- Client PII is exchanged through the Firm's secure client portal (SmartVault). When a password protects a file, it is given by phone or text, never in the same email.
- PII is disclosed only to the client, to parties the client authorized in writing, to taxing authorities, and to service providers that need it to do their work.
- Callers and emailers asking for client information are verified before anything is released. Requests to change a client's bank account or address are confirmed by calling the client at a number already on file.
- Records taken out of the office are kept to the minimum, never left unattended in a vehicle, and returned as soon as possible.

4.12 Backup and recovery

Client data is backed up using encrypted cloud backup, nightly. At least one copy is kept off site. A test restore is performed at least once a year, before tax season.

5. Testing and Monitoring

The Firm regularly tests or monitors whether its key safeguards work, including controls that detect attacks and intrusions (16 CFR 314.4(d)(1)).

Information systems are under continuous monitoring by First Coast IT Services, which detects changes and new vulnerabilities on an ongoing basis (16 CFR 314.4(d)(2)). Alerts go to the Qualified Individual.

Routine checks:

Check	How often	Who
E-file counts in IRS e-Services compared with returns actually filed	Weekly during filing season, monthly otherwise	Marcus Hill
Security updates installed on every device	Monthly	Marcus Hill
Sign-in and audit log review	At least every 90 days	First Coast IT Services
Access list (Attachment F) matches current staff	Quarterly and when staff change	Marcus Hill
Backup restore test	Annually, before tax season	First Coast IT Services
Phishing awareness check (simulated email or quiz)	Annually	Marcus Hill

6. Personnel, Training and Accountability

- Every owner, employee, seasonal worker and contractor with access to PII completes security awareness training before access is granted and again every December (16 CFR 314.4(e)(1)). Training covers this plan, the rules in Attachment B, phishing and phone scams, and how to report an incident. Training is updated to reflect risks found in the risk assessment.
- Each person signs the acknowledgment in Attachment D after training. Signed copies are kept on file.
- The Firm uses qualified people to manage security: Marcus Hill, supported by First Coast IT Services (16 CFR 314.4(e)(2)).
- The Qualified Individual keeps current on threats by subscribing to IRS e-News for Tax Professionals and IRS QuickAlerts and reviewing Security Summit alerts, and completes security training each year (16 CFR 314.4(e)(3)–(4)).
- Background checks are completed for new hires who will access PII.
- Staff and contractors who handle PII sign a confidentiality agreement.
- Anyone who willfully discloses PII or ignores this plan faces discipline up to and including termination.
- When someone leaves: all accounts are disabled the same day (tax software, email, portal, e-Services, remote access); keys, badges and devices are returned; shared codes such as alarm or door codes are changed.

7. Service Provider Oversight

- Before hiring any provider that will access client information, the Qualified Individual confirms the provider can maintain appropriate safeguards (16 CFR 314.4(f)(1)).
- Each such provider is required by contract to implement and maintain those safeguards (16 CFR 314.4(f)(2)).

- Providers are reassessed at least once a year, based on the risk they present (16 CFR 314.4(f)(3)). Results are recorded in Attachment G.
- Tax software vendors and e-file transmitters are bound by IRS Publication 1345 and are still listed in Attachment G.

8. Program Evaluation and Annual Report

8.1 Evaluation and adjustment

The Firm updates this plan based on testing and monitoring results, material changes to operations or business arrangements, new risk assessments, and any other circumstance that could materially affect security (16 CFR 314.4(g)). A full review happens every November. Changes are recorded in Attachment H, and staff are told in writing when the plan changes.

8.2 Annual written report

At least once a year the Qualified Individual gives Denise Carter, Owner, Enrolled Agent, a written report covering (16 CFR 314.4(i)):

- The overall status of the information security program and the Firm's compliance with the Safeguards Rule.
- Material matters: risk assessment results, risk management and control decisions, service provider arrangements, testing results, security events and how they were handled, and recommended changes.

9. Incident Response Plan

This written incident response plan meets 16 CFR 314.4(h). It applies to any security event that materially affects the confidentiality, integrity or availability of client information. Attachment C is the one-page checklist for use during an incident.

9.1 Goals

- Stop the incident and secure systems quickly.
- Protect clients from tax-related identity theft and fraudulent returns.
- Meet every notification duty on time.
- Fix the weakness so it does not happen again.

9.2 Roles and decision authority

Role	Person	Authority
Incident lead	Marcus Hill	Declares an incident, directs containment, contacts the IRS, law enforcement, vendors and insurer
Spokesperson (PIO)	Denise Carter	Approves and makes all statements to clients, media and the public

Role	Person	Authority
Owner	Denise Carter	Approves spending, legal counsel, and client notification decisions
IT support	First Coast IT Services	Containment, forensic preservation, restoration

9.3 Internal process

- Report: anyone who suspects an incident tells the Qualified Individual at once. Signs include e-filed returns rejected as duplicates, clients receiving IRS letters about returns they did not file, more e-file submissions in e-Services than the Firm sent, computers acting on their own, or locked-out accounts.
- Contain: disconnect affected devices from the network (do not turn them off), disable compromised accounts, change passwords from a clean device, and stop e-filing until the tax software provider confirms it is safe.
- Preserve: keep logs, emails and affected devices for investigators. Do not wipe or rebuild until the insurer and investigators agree.
- Assess: determine what data, which clients and what time period were involved, and whether 500 or more consumers are affected.
- Notify: follow Section 9.4.
- Recover: restore from clean backups, reset credentials, and confirm systems are clean before returning to normal work.

9.4 Communications and notifications

External notifications (call the IRS first — speed lets the IRS block fraudulent returns):

Who	How	When
IRS Stakeholder Liaison for Florida	Find the local liaison at irs.gov (search "Stakeholder Liaison local contacts"). IRS toll-free lines cannot take third-party reports.	Immediately
State tax agencies	Email StateAlert@taxadmin.org for state reporting instructions	Immediately
Florida Attorney General	Per state breach-notification law; most states require it	As state law requires
FBI	Internet Crime Complaint Center (ic3.gov) or the local field office	Promptly
Local police	File a report	Promptly
Federal Trade Commission	Safeguards Rule security event reporting form on ftc.gov (Section 10)	Within 30 days if 500+ consumers
Tax software provider: Drake Tax	Support line	Immediately
Portal, website and cloud providers	Reset access and review their logs	Immediately

Who	How	When
Cyber insurance carrier: Cyber liability policy (agent: Coastal Insurance Group)	Claims line; many policies require notice before outside help is hired	Immediately
Legal counsel	Advice on notification duties	Promptly
Affected clients	Written notice from the PIO; advise an IRS Identity Protection PIN and, if applicable, Form 14039	As required by law and advised by counsel

Internal communications go through the Qualified Individual. Staff do not discuss the incident with clients or outsiders unless the PIO approves.

9.5 Remediation

The Qualified Individual identifies the weaknesses in systems and controls that allowed the incident, sets a fix and a deadline for each, and confirms each fix is complete.

9.6 Documentation and reporting

The Qualified Individual keeps a written record of each security event: timeline, what was affected, decisions made, notifications sent (with dates) and remediation completed. The record is included in the next annual report.

9.7 Post-incident review

Within 30 days after an incident is closed, the Qualified Individual reviews what happened and revises this plan and the incident response plan as needed.

10. FTC Notification Requirement

If a notification event involves the information of at least 500 consumers, the Firm notifies the FTC as soon as possible and no later than 30 days after discovery, using the electronic form on the FTC's website (16 CFR 314.4(j)). An event is treated as discovered on the first day it is known to any employee, officer or agent of the Firm other than the person who committed the breach. The notice includes:

- The Firm's name and contact information.
- The types of information involved.
- The date or date range of the event, if it can be determined.
- The number of consumers affected or potentially affected.
- A general description of the event.
- Whether a law enforcement official has determined in writing that public notice would impede a criminal investigation or harm national security, and how the FTC can contact that official.

11. Corrective Action Plan

These gaps were identified when this plan was prepared. The Qualified Individual tracks each one to completion and records the date it is closed.

Gap	Action	Target date	Done
One or more service providers that touch client data have no written security terms.	Get a contract, data protection addendum or written security commitment from each provider listed in Attachment G (16 CFR 314.4(f)(2)).	February 13, 2027	☐

Implementation and Signatures

Effective November 15, 2026, Riverside Tax & Bookkeeping LLC adopts this Written Information Security Plan in compliance with the Gramm-Leach-Bliley Act and the Federal Trade Commission Safeguards Rule (16 CFR Part 314), and any applicable requirements of Florida law. A copy of this plan is stored off site or in secure cloud storage in case of disaster.

Signature: _____ Date: _____
Denise Carter, Owner, Enrolled Agent

Signature: _____ Date: _____
Marcus Hill, Qualified Individual

> This plan was prepared from the Firm's own answers using Tax Pro WISP Builder. It is a compliance template, not legal advice. The Firm is responsible for confirming the plan matches its actual practices and for meeting any additional state requirements.

Attachment A — Record Retention and Disposal Schedule

Record type	Format	Keep for	Disposal method
Client tax returns and workpapers	Electronic / paper	4 years after filing	Secure deletion; cross-cut shred
Client source documents (W-2, 1099, ID copies)	Electronic / paper	Return to client or keep with workpapers	Secure deletion; cross-cut shred
Section 7216 consents and engagement letters	Electronic / paper	4 years	Secure deletion; cross-cut shred
Employee personnel and payroll records	Electronic / paper	As employment law requires	Secure deletion; cross-cut shred
Training acknowledgments (Attachment D)	Paper / electronic	Duration of employment + 3 years	Cross-cut shred
Incident records and annual reports	Electronic	5 years	Secure deletion
Retired hard drives, phones and USB drives	Device	Until wiped or destroyed	Certified wipe or physical destruction

Information not needed for business operations or required by law is disposed of no later than two years after its last use for the client (16 CFR 314.4(c)(6)). This schedule is reviewed every November.

Attachment B — Rules of Behavior for Safeguarding Client Data

Post these rules where staff work. Everyone follows them, including owners.

- Lock your screen whenever you step away. Keep desks clear of client papers when you are not at them, and lock papers away at the end of the day.
- Never share your password or MFA codes. No one from the Firm, the IRS, or a software company will ever ask for them.
- Do not click links or open attachments you were not expecting. If a message seems important, call the sender at a number you already have.
- Before releasing client information or changing bank or address details, verify the request by calling the client at the number on file.
- Send client files only through the client portal. Never put PII in the body of an email or text.
- Use only Firm-approved devices and accounts for client work. No client data on personal phones, home computers, personal email or personal cloud storage.
- Do not plug in unknown USB drives or install software without approval from the Qualified Individual.
- Use strong, unique passwords of at least 12 characters, and never reuse a Firm password anywhere else.
- Never leave laptops, phones or files unattended in a car or public place.
- Report anything suspicious to Marcus Hill right away — a strange email, a lost device, a client who received an unexpected IRS letter. Reporting fast is never a mistake.

Attachment C — Incident Response Checklist

Use this page during an incident. Check off each step and write the time.

✔	Step	Time / notes
☐	Tell the Qualified Individual (Marcus Hill, (904) 555-0143)	
☐	Disconnect affected devices from the network — do not turn them off	
☐	Disable compromised accounts; change passwords from a clean device	
☐	Stop e-filing; call the tax software provider	
☐	Call the IRS Stakeholder Liaison for Florida (find at irs.gov)	
☐	Email StateAlert@taxadmin.org for state reporting steps	
☐	Call the cyber insurance carrier before hiring outside help	
☐	Preserve evidence: logs, emails, devices — do not wipe	
☐	Check e-Services e-file counts against returns actually sent	
☐	Report to FBI (ic3.gov) and local police	
☐	Notify the Florida Attorney General as state law requires	
☐	Count affected consumers. 500 or more: file the FTC report within 30 days of discovery	
☐	PIO sends client notices; advise IP PIN and Form 14039 where applicable	
☐	Restore from clean backups; reset all credentials	
☐	Write the incident record; review and update this plan within 30 days	

Attachment D — Employee and Contractor Acknowledgment (Training Sign-off)

I acknowledge that I have received and read the Written Information Security Plan of Riverside Tax & Bookkeeping LLC and the Rules of Behavior in Attachment B. I completed security training conducted by the Qualified Individual and had my questions answered. I understand that I must protect the personally identifiable information of clients, employees and contacts, that I must report any suspected incident immediately, and that failure to follow this plan may lead to discipline up to and including termination. I understand that training and this acknowledgment are repeated each year.

Name	Title / role	Training date	Signature

Attachment E — Hardware and Data Inventory

Every device, storage location and service that holds or processes client PII. Update when equipment is added or retired.

Item	Location	Primary user	Data stored or processed	In service	Last checked
Office desktop (Denise)	Front office	Denise Carter	Tax software, client files, email		
Laptop (Marcus)	Office / travels	Marcus Hill	Email, portal, QuickBooks		
Seasonal workstation	Back office	Alicia Gomez	Tax software		
Network router / firewall	Storage closet	IT provider	All network traffic		
Multifunction printer/scanner	Front office	All staff	Scanned client documents		

Attachment F — Personnel Authorized to Access Client Data

Name	Role and duties	Access level	Date granted	Date removed
Denise Carter	Owner / preparer	All client data	January 2, 2019	
Marcus Hill	Office manager / QI	All client data	June 1, 2021	
Alicia Gomez	Seasonal preparer	Tax software, assigned clients	January 5, 2026	
Tom Reyes	Front desk	Scheduling, portal uploads	January 6, 2025	

When a person's access changes, end the old line with a removal date and add a new line. This keeps a clear record of who had access and when.

Attachment G — Service Provider Register

Provider	Service	Client data it can access	Security terms in contract	Last reviewed
Drake Software	Tax software / e-file	All return data	Yes	
SmartVault	Client portal	Client documents	Yes	
First Coast IT Services	IT support and monitoring	Systems access	Yes	
Bold City Shredding	Document shredding	Paper records	No — see Corrective Action Plan	

Attachment H — Annual Review and Qualified Individual Report Log

Record each annual review, each written report to the owner, and each change to this plan.

Date	Type (review / report / change)	Summary of findings or changes	Signed
November 15, 2026	Plan adopted	Initial version 2.0 prepared with Tax Pro WISP Builder	

Attachment I — Safeguards Rule Compliance Map

Each element of 16 CFR 314.4, where this plan covers it, and its status when the plan was prepared. Readiness: **94%** (16 of 17 elements in place, 1 with open corrective actions). Firms with information on fewer than 5,000 consumers are exempt from 314.4(b)(1), (d)(2), (h) and (i) under 16 CFR 314.6; this firm keeps them as best practice.

Element	Requirement	Where in plan	Status	Basis
314.4(a)	Designate a Qualified Individual	Section 2.1	Met	Marcus Hill, Office Manager
314.4(b)	Written risk assessment	Section 3	Met (best practice)	Not required under 5,000 consumers (314.6); the plan keeps it.
314.4(c)(1)	Access controls, least privilege	Section 4.1, Attachment F	Met	4 authorized people listed
314.4(c)(2)	Data and systems inventory	Section 4.2, Attachment E	Met	5 devices inventoried
314.4(c)(3)	Encrypt client data at rest and in transit	Sections 4.3, 4.11	Met	Disk encryption on; documents move by secure portal.
314.4(c)(4)	Secure practices for applications	Section 4.4	Met	Commercial software (Drake Tax) kept current; no in-house code.
314.4(c)(5)	Multi-factor authentication	Section 4.5	Met	Authenticator app
314.4(c)(6)	Secure disposal (within 2 years of last use)	Section 4.6, Attachment A	Met	Keep 4 years, then shredding service.
314.4(c)(7)	Change management	Section 4.7	Met	Changes approved by the Qualified Individual and logged in Attachment H.
314.4(c)(8)	Monitor and log user activity	Section 4.8	Met	Account activity and e-file counts reviewed.
314.4(d)	Continuous monitoring, or yearly pen test + scans every 6 months	Section 5	Met	Continuous monitoring in place.
314.4(e)	Security awareness training	Section 6, Attachment D	Met	Every December, with signed acknowledgments.
314.4(f)	Oversee service providers	Sections 7, 11	Gap: see Section 11	Bold City Shredding: no written security terms yet.
314.4(g)	Evaluate and adjust the program	Section 8.1	Met	Reviewed every November.
314.4(h)	Written incident response plan	Section 9, Attachment C	Met (best practice)	Not required under 5,000 consumers (314.6); the plan keeps it.
314.4(i)	Annual written report to the owner	Section 8.2, Attachment H	Met (best practice)	Not required under 5,000 consumers (314.6); the plan keeps it.
314.4(j)	Notify the FTC within 30 days (500+ consumers)	Section 10	Met	Steps and required contents written in.