Written Information Security Plan

Cascade Ridge Tax Group LLC

Version: 1.0 **Adopted:** November 12, 2026 **Last reviewed:** November 12, 2026 **Next scheduled review:** October 2027 (before the start of PTIN renewal season) **Qualified Individual:** Morgan Ellis, Owner (see §3)

> **How to read this plan.** This plan was completed with facts about this firm from its intake answers before it was issued. A control is written into this plan only when it is in place and verified or attested by the owner. Anything not yet in place appears in the firm's Gap List (§16 and the evidence binder), with a fix and a date — never in this plan as if it were fact. Notes marked **Small-firm position** explain how 16 CFR 314.6 changes the requirement for firms that maintain customer information concerning fewer than 5,000 consumers. This plan keeps those elements in place and documented rather than deleting them, and each note says why.

WispTrust client reference: WT-1192

1. Purpose, scope, and legal basis

1.1 Purpose

This Written Information Security Plan ("the Plan") describes how Cascade Ridge Tax Group LLC ("the Firm") protects the security, confidentiality, and integrity of customer information, and how the Firm protects against anticipated threats and unauthorized access that could result in substantial harm or inconvenience to any customer. These are the objectives stated in 16 CFR 314.3(b).

1.2 Legal basis

The Firm is a "financial institution" under the Gramm-Leach-Bliley Act because it is in the business of completing income tax returns (16 CFR 314.2(h)(2)(viii); "tax preparation firms" are listed at 16 CFR 314.1(b)). Under 16 CFR 314.3(a), the Firm must develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards appropriate to the Firm's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

IRS Publication 5708, Creating a Written Information Security Plan for your Tax & Accounting Practice (Rev. 8-2024), states that this requirement applies to tax and accounting professionals **regardless of size**, and this Plan follows Publication 5708's outline. IRS Publication 4557,

Sample — fictional firm shown. © 2026 MVP Forge LLC. Your plan is built from your firm's own answers.

Safeguarding Taxpayer Data: A Guide for Your Business (Rev. 6-2024), explains the safeguards the IRS expects.

Each paid preparer at the Firm acknowledges the duty every year: IRS Form W-12 (PTIN application/renewal), line 11, requires the applicant to confirm awareness that paid tax return preparers are required by law to create and maintain a written information security plan.

1.3 Scope

This Plan covers all customer information the Firm receives, creates, stores, transmits, or disposes of, in every format — electronic, paper, and spoken — and every person, device, system, and facility that touches it, including work performed from home offices and seasonal work locations listed in Appendix B.

1.4 Definitions

- **Customer information** — any record containing nonpublic personal information about a customer of the Firm, in any format, handled by the Firm or its service providers (16 CFR 314.2). A consumer becomes a customer when they become the Firm's client for tax preparation services (16 CFR 314.2(e)(2)(i)(H)).
- **Information system** — any system, software, device, or network used to access, store, or transmit customer information.
- **Security event** — an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on it, or the Firm's electronic communications network.
- **Notification event** — unauthorized acquisition of unencrypted customer information (see §13).
- **Qualified Individual (QI)** — the individual designated under §3 of this Plan (16 CFR 314.4(a)).

2. Firm profile

Item	Detail
Legal name	Cascade Ridge Tax Group LLC
Trade name (if any)	Cascade Ridge Tax Group
Principal office	2214 Chapman Highway, Suite 8, Knoxville, TN 37920
Other work locations	Home office and office
Owner(s)	Morgan Ellis
Staff (all roles)	2 — see Appendix A
Consumers whose information the Firm maintains	Approximately 2800 — including former clients whose records are still stored
Firm's position under 16 CFR 314.6	Fewer than 5,000 consumers — see the Small-firm position notes throughout this Plan
Tax software used	ProSeries Professional (desktop)

Sample — fictional firm shown. © 2026 MVP Forge LLC. Your plan is built from your firm's own answers.

System / data	At rest	In transit	Evidence checked (date)
Professional, desktop)			
Client portal (SmartVault)	Vendor encryption statement to be filed in the evidence binder — see the Gap List	TLS (vendor platform)	Intake attestation — verification during the in-house review
Email (Microsoft 365)	Provider service encryption	TLS; sensitive attachments sent via portal only	Intake attestation — verification during the in-house review
Backups (Cloud backup service (fictional vendor))	Encrypted (attested)	Encrypted (attested)	Intake attestation — verification during the in-house review

Where the QI determines encryption of a specific item is infeasible, the Firm uses effective alternative compensating controls **reviewed and approved in writing by the QI**. Exceptions in force at generation: none recorded. Any future exception is recorded here with the QI's signature and date.

The Firm's baseline device protections follow the IRS "Security Six" (Publication 4557): anti-virus/anti-malware (EDR/anti-malware with automatic updates (product name on file)) on all devices with automatic updates; firewall; multi-factor authentication (§6.4); backup software/services (§6.8); drive encryption (this section); and a VPN for remote access (§6.9).

6.3 Secure development and application vetting — 314.4(c)(4)

The Firm does not develop software in-house. Before adopting any externally developed application that will transmit, access, or store customer information, the Firm evaluates its security: the vendor's published security practices, whether it supports multi-factor authentication, its encryption statements, and any available independent assurance (for example, a SOC 2 report). The evaluation is recorded in Appendix F before the application is put into use.

6.4 Multi-factor authentication — 314.4(c)(5)

The Firm implements multi-factor authentication for any individual accessing any information system. MFA uses at least two of: something the user knows, something the user has, or something the user is (16 CFR 314.2(k)).

The current MFA register is Appendix D. It covers, per the firm's intake answers: Email (Microsoft 365), Tax software (ProSeries Professional), Client portal (SmartVault), Banking, Cloud storage (SmartVault), Remote access, Password manager (1Password).

Exceptions in force at generation: none. Any future exception requires the QI to approve in writing the use of reasonably equivalent or more secure access controls, recorded in Appendix D.

Sample — fictional firm shown. © 2026 MVP Forge LLC. Your plan is built from your firm's own answers.

Gap List at adoption: 12 items (2 gaps, 6 confirmations, 0 contradictions, 2 per-client completions, 2 review items), filed in the evidence binder, each with an owner and a due date recorded at the in-house review.

Adoption statement — Qualified Individual. "I adopt this Plan as the Firm's Qualified Individual under 16 CFR 314.4(a). The factual statements in it are true of the Firm, as verified with the preparer on the date signed below."

Firm	Cascade Ridge Tax Group LLC
Qualified Individual (print)	Morgan Ellis, Owner
Date of verification (in-house review)	_____

Appendices

Appendix A — Authorized users and access matrix (314.4(c)(1); Pub 5708 Attachment F)

Name	Role	Systems accessible	Access level	Date granted	Date ended	MFA enrolled
Morgan Ellis	Owner / Preparer	All systems	Admin	At adoption	—	Y
Casey Ellis	Seasonal preparer (December–April)	ProSeries Professional, client portal, email	Standard user	At adoption	—	Y

Appendix B — Hardware and device inventory (314.4(c)(2); Pub 5708 Attachment E)

Device (make/ model)	Serial/ asset tag	Location	Used by	Information stored/ processed	Encryption status
Dell OptiPlex workstation	DT-01	Office	Owner (Morgan Ellis)	Tax return data (ProSeries data file)	Full-disk encryption ON (attested)
Lenovo ThinkPad laptop	LT-01	Office / home office	Owner (Morgan Ellis)	Tax return data (SmartVault sync folder, email)	Full-disk encryption ON (attested)
HP LaserJet printer/scanner	PR-01	Office workroom	Owner (Morgan Ellis)	Printed client documents; scans to SmartVault	Full-disk encryption ON (attested)

Appendix C — Systems and data map (314.4(c)(2))

System / service	Purpose	Customer information held	Hosted where	Administered by
ProSeries Professional				Morgan Ellis

Sample — fictional firm shown. © 2026 MVP Forge LLC. Your plan is built from your firm's own answers.

Generated by the WispTrust generator (MVP Forge LLC) from the firm's intake answers on November 12, 2026. Documentation support and general information — not legal, tax, or security-engineering advice. Have your attorney review this plan for your firm's circumstances.

Basis & Sources

This plan is built on the FTC Safeguards Rule itself — Standards for Safeguarding Customer Information, 16 CFR Part 314 — and is structured following the Internal Revenue Service's own guidance for tax professionals: Publication 4557, Safeguarding Taxpayer Data (Rev. 6-2024), and Publication 5708, Creating a Written Information Security Plan for Your Tax & Accounting Business. Incident-reporting clocks for e-file providers follow IRS Publication 1345. Nothing in this plan rests on a secondary summary where a primary source exists.

How the parts of this plan map to the rule:

Part of this plan	Safeguards Rule paragraph it answers	IRS guidance followed
Qualified Individual designation (§3)	16 CFR 314.4(a)	IRS Publications 4557 and 5708
Risk assessment (§4)	16 CFR 314.4(b)	IRS Publication 5708
Access controls and physical safeguards (§6)	16 CFR 314.4(c)(1)	IRS Publication 4557
Encryption of customer information (§6)	16 CFR 314.4(c)(3)	IRS Publication 4557
Secure development and application evaluation (§6)	16 CFR 314.4(c)(4)	IRS Publication 5708
Multi-factor authentication (§6 and Appendix D)	16 CFR 314.4(c)(5)	IRS Publication 4557
Secure disposal and retention (§6 and Appendix E)	16 CFR 314.4(c)(6)	IRS Publication 4557
Testing of safeguards (§7)	16 CFR 314.4(d)	IRS Publication 5708
Staff security training (§9)	16 CFR 314.4(e)(1)	IRS Publication 4557
Service-provider oversight (§10 and Appendix F)	16 CFR 314.4(f), including (f)(2) contract safeguards	IRS Publication 5708
Annual review and program updates (§11)	16 CFR 314.4(g)	IRS Publication 5708
Qualified Individual's annual report (§12)	16 CFR 314.4(i)	IRS Publication 5708
Incident response (§8 and the companion Incident Response Plan)	16 CFR 314.4(h)	IRS Publications 1345 and 5708
FTC notification of a notification event (Incident Response Plan §6.3)	16 CFR 314.4(j)	FTC Safeguards Rule materials at ftc.gov
Small-firm position, where stated (firms under 5,000 consumers)	16 CFR 314.6	eCFR text of Part 314
State breach-notification matrix (§14)	Researched state statutes for the states listed in §14	The state sources cited in §14 itself

Sample — fictional firm shown. © 2026 MVP Forge LLC. Your plan is built from your firm's own answers.