Written Information Security Plan (WISP)

HC1 Ventures LLC dba HC1 Tax

Prepared for: Enoch Wright

Effective date: January 01, 2026 | Version: 1.0 (Living Document)

Business legal name: HC1 Ventures LLC

Doing business as (DBA): HC1 Tax

Business address (mailing): 807 4th St NW, New Philadelphia, OH 44663

Website: hc1.tax

Workforce size: 2-person LLC

Operating model: Remote / no public-facing physical office

Primary client portal: Financial Cents Client Portal (app.financial-cents.com)

Tax preparation software: TaxAct Professional (TaxAct Pro)

Primary work device: Encrypted laptop (full-disk encryption)

Backups: Encrypted backups stored in Backblaze B2

Payments: Financial Cents billing/payments + Novo Bank

1. Purpose, Scope, and Regulatory Basis

This Written Information Security Plan (WISP) documents the administrative, technical, and physical safeguards used by HC1 Tax to protect customer information and taxpayer data throughout its lifecycle. This plan is designed to be practical for a small, remote practice while meeting professional obligations.

Regulatory and guidance sources informing this plan include the Federal Trade Commission (FTC) Safeguards Rule (16 CFR Part 314) and IRS security guidance for tax professionals (including IRS Publication 5708 and Publication 4557).

1.1 Definitions

- Customer information / taxpayer data: Any information provided by or about a client or taxpayer, including tax returns, source documents, identifying information (e.g., SSN/ITIN), financial records, and authentication data.

- Information system: Any system, device, application, or cloud service used to create, receive, store, process, transmit, or dispose of customer information.
- Qualified Individual (QI): The person designated to oversee and implement this information security program.

1.2 Scope

- Applies to all personnel (employees, owners, contractors) with access to customer information.
- Applies to all customer information in any form: electronic, paper, and verbal communications.
- Applies to all systems used by HC1 Tax including laptops, cloud services, portals, backups, and financial systems.

2. Information Security Governance

2.1 Qualified Individual and Roles

The following roles apply for this 2-person organization:

Role	Person / Backup	Primary Responsibilities
Qualified Individual (QI)	Enoch Wright (backup: Samantha Wottle)	Oversees the WISP, ensures implementation, approves risk treatment decisions, coordinates incident response, and manages vendor/security reviews.
System Administrator (internal)	Enoch Wright	Device security, access control, patching, backups, and account lifecycle management.
Privacy & Records Lead	Enoch Wright (backup: Samantha Wottle)	Client intake/disclosure controls, retention/offboarding actions, secure disposal, and documentation.

2.2 Policy Management and Review

- This WISP is reviewed at least annually and whenever there are material changes (new systems, new vendors, security incidents, major workflow changes).
- Changes are documented in the Version History table in Appendix A.

3. Data Inventory and Data Flows

3.1 Types of Customer Information Handled

- Tax return data: federal/state filings, e-file acknowledgments, prior-year returns.
- Source documents: W-2/1099s, K-1s, brokerage statements, bank statements, receipts, identity documents (if provided).
- Client communications: messages through portal, email, phone notes.
- Payment information: invoices, payment confirmations, transaction records (card/ACH data handled by payment processor).

3.2 Systems and Storage Locations

System / Location	Purpose	Data Stored/Processed	Key Safeguards (summary)
Financial Cents Client Portal	Client intake, secure file exchange, messaging, billing/payments workflow	Uploaded client documents, messages, requests, billing artifacts	Encrypted in transit/at rest, role-based access, SOC 2 compliance (per provider).
TaxAct Professional	Prepare, store, and transmit tax return data	Return data, e-file transmissions, client records	Encrypted transmission (SSL/TLS), account security controls, vendor monitoring (per provider).
Encrypted Laptop	Primary workstation	Working copies of documents/returns, local caches	Full-disk encryption, strong authentication, anti-malware, patching, locked screen.
Backblaze B2 (encrypted backups)	Backup and recovery	Encrypted backup archives of working data	AES-256 server-side encryption options; client-side encryption for backups; access controls.
Novo Bank	Business banking	Banking records, transaction metadata	FDIC-insured deposits via partner bank; bank-level encryption (per provider).

3.3 High-Level Data Flow (Narrative)

1. Client provides documents and information through the Financial Cents client portal (preferred).
2. HC1 Tax downloads or accesses documents as needed and prepares returns in TaxAct Pro on an encrypted laptop.
3. TaxAct Pro transmits returns to the IRS/state agencies using encrypted connections (per vendor).
4. Working files and final deliverables are stored per retention policy; encrypted backups are maintained in Backblaze B2.
5. Clients receive copies of deliverables; upon client offboarding, HC1 Tax provides confirmation of deletion per the offboarding procedure (Section 8).

4. Risk Assessment

HC1 Tax performs a risk assessment to identify reasonably foreseeable internal and external risks to customer information. Given a small remote practice, the primary risk drivers include phishing, account takeover, ransomware, device loss/theft, misdirected disclosures, weak vendor controls, and improper retention/disposal.

4.1 Risk Assessment Method

- Identify assets (systems, accounts, data stores).
- Identify threats and vulnerabilities (phishing, malware, weak passwords, misconfiguration, physical loss).
- Assess likelihood and impact (Low/Medium/High).
- Select controls and document risk treatment (mitigate, transfer, accept, avoid).
- Reassess annually and after material changes or incidents.

4.2 Top Risks and Controls (Summary Table)

Risk	Likelihood	Impact	Primary Controls
Phishing / credential theft (portal, email, TaxAct, banking)	High	High	MFA, phishing training, password manager, verified portal use, least privilege.
Ransomware/malware on workstation	Medium	High	Endpoint protection, patching, limited admin rights, offline/immutable backups, restore testing.
Lost or stolen laptop	Medium	High	Full-disk encryption, strong login, auto-lock,

			remote wipe, minimal local storage.
Unauthorized access by insider / overprivileged accounts	Low-Med	High	Role-based access, unique accounts, access reviews, separation of duties.
Vendor breach (Financial Cents, Backblaze, TaxAct, payment processor)	Medium	High	Vendor due diligence, SOC reports (when available), contract/DPAs, strong account controls, incident notifications.
Improper retention/disposal leading to unnecessary exposure	Medium	Medium-High	Retention schedule, secure deletion standards, documented offboarding, periodic purge checks.

5. Safeguards

5.1 Administrative Safeguards

Access management

- Unique user accounts for each team member for each system.
- Principle of least privilege: access is granted only as needed for job duties.
- Quarterly access review: confirm active users, roles, and permissions for each critical system (Financial Cents, TaxAct, Backblaze, banking).
- Immediate access removal for departing personnel.

Security awareness and training

- Initial training upon hiring: phishing, safe handling of taxpayer data, secure portal usage, incident reporting.
- Quarterly refresher training and simulated phishing or tabletop exercises.
- Document completion in a Training Log (Appendix E).

Policies and procedures

- Acceptable use policy for devices and accounts (no shared logins, no personal devices unless approved and secured).
- Clean desk / screen policy for any at-home workspace.

- Secure communication policy: use portal for sensitive documents; avoid sending taxpayer data via unencrypted email.

5.2 Technical Safeguards

Workstation and device security

- Full-disk encryption enabled on all work laptops.
- Strong device login (minimum 12-character passphrase) and automatic screen lock (<= 10 minutes).
- Automatic operating system and application updates (patching) enabled.
- Reputable anti-malware/endpoint protection installed and kept current.
- Separate standard user accounts for daily work; admin credentials used only when necessary.

Authentication and account security

- Multi-factor authentication (MFA) enabled wherever available for: Financial Cents, TaxAct accounts, Backblaze/B2 access, email accounts used for business, and Novo banking.
- Password manager required for storing and generating unique passwords.
- No reuse of passwords across systems; minimum password length 14 characters where configurable.
- Account recovery information (phone/email) is controlled by the Qualified Individual.

Encryption and secure transmission

- TaxAct uses encrypted transmission for return data sent to TaxAct/IRS (per vendor).
- Portal use required for sensitive document exchange whenever possible.
- Backups are encrypted before upload; encryption keys are stored securely (password manager + offline recovery method).

Backup and recovery

- Encrypted backups are stored in Backblaze B2.
- Backups are performed at least daily during filing season and weekly otherwise.
- Monthly restore test of a sample backup to validate recovery and document results.
- Backup retention: maintain at least 180 days of versioned backups.

Logging and monitoring

- Enable and review security logs/alerts available in critical systems (Financial Cents, TaxAct, Backblaze, banking) for suspicious logins or access.
- Configure real-time alerts where available (new device sign-in, failed login spikes, payment anomalies).
- Maintain an Incident & Alert Log (Appendix F).

5.3 Physical Safeguards (Remote Practice)

- Work devices are not left unattended in public; use privacy screen when working outside home.
- Paper documents (if any) are stored in a locked container; minimize printing.
- Secure disposal: cross-cut shredding or certified shredding service for any paper containing taxpayer data.

- Device disposal: wipe or destroy storage media before recycling/sale (Appendix G disposal checklist).

6. Vendor and Service Provider Management

HC1 Tax uses third-party service providers that may access, transmit, process, or store customer information. HC1 Tax will select, retain, and oversee providers capable of maintaining appropriate safeguards.

6.1 Provider Due Diligence Requirements

- Maintain a vendor inventory (Appendix D) including: purpose, data types involved, security features, and account owner.
- Review vendor security documentation at onboarding and annually (e.g., security pages, SOC reports when available, compliance statements).
- Ensure contracts/terms provide for confidentiality, security, and breach notification where possible.
- If a vendor cannot support required safeguards, implement compensating controls or replace the vendor.

6.2 Key Providers (Current)

Financial Cents

- Use as the primary portal for client document exchange and communications.
- Use role-based access controls and restrict team permissions.
- Enable available authentication protections; review the vendor security documentation and SOC attestation (where available).

TaxAct Professional (TaxAct Pro)

- Limit access to authorized staff only; use MFA and strong passwords.
- Prefer vendor-supported secure transmission methods for filings.

Backblaze B2

- Backups are encrypted prior to upload.
- Restrict API keys and access tokens; rotate credentials annually or upon suspected compromise.

Novo Bank and payments

- Use Novo for business banking; enable 2FA where offered.
- Payments are processed through Financial Cents and its payment provider.

7. Incident Response Plan

7.1 What Constitutes a Security Incident

- Suspected phishing success or credential compromise.
- Unauthorized access to client portal, tax software accounts, backup storage, or banking.

- Malware/ransomware infection.
- Lost or stolen device with potential access to customer information.
- Accidental disclosure (mis-sent file, wrong recipient).
- Vendor breach notification involving HC1 Tax data.

7.2 Immediate Response Steps (First 0-24 Hours)

6. Ensure safety; stop the bleeding: disconnect affected device(s) from the internet if malware is suspected.
7. Preserve evidence: do not wipe systems unless required to contain ongoing harm; document what happened.
8. Notify the Qualified Individual and initiate the Incident Log (Appendix F).
9. Reset compromised credentials and rotate affected API keys/tokens; force logout sessions where possible.
10. Engage vendors (Financial Cents, TaxAct, Backblaze, bank) to lock accounts and review access logs.
11. If ransomware: isolate systems, assess backup integrity, and begin recovery from clean backups.

7.3 Notification and Reporting (As Applicable)

- Assess whether customer information was accessed or exfiltrated; determine affected individuals and data elements.
- Consult legal counsel and/or cyber insurance provider if available.
- Follow IRS and state requirements for reporting and client notification as applicable.
- If e-file data is compromised, follow IRS guidance for tax professionals and consider contacting the IRS Stakeholder Liaison for assistance.

7.4 Post-Incident Review

- Root cause analysis and remediation plan within 14 days of incident closure.
- Update safeguards and this WISP based on lessons learned.
- Conduct a tabletop exercise annually.

8. Data Retention, Disposal, and Client Offboarding

8.1 Retention Policy (Current Practice)

HC1 Tax retains client files for 7 years after the end of the tax year for which services were provided (or 7 years after the end of the engagement, whichever is later), unless a documented exception applies (e.g., open audit/appeal, litigation hold, or written client request for extended retention). After the retention period expires, data is securely disposed of according to Section 8.3 and documented in the Disposal/Offboarding logs.

8.2 Retention Schedule (Adopted)

HC1 Tax retention schedule:

- Tax returns and supporting records (workpapers/source docs relied upon): retain 7 years.

- Engagement letters, consents, and communications required to document services: retain 7 years.
- Client identity documentation (if collected): retain only as long as necessary for identity verification and compliance; default to delete within 90 days after filing unless legally required longer.
- Payment and accounting records (invoices, receipts, transaction confirmations): retain 7 years; do not store full card numbers locally.
- Exceptions: extend retention only with a documented reason (audit, dispute, litigation hold, or written client request).

8.3 Secure Disposal Standards

- Electronic deletion uses secure methods appropriate to the storage medium (cryptographic erasure where available, secure wipe for local media).
- Paper is cross-cut shredded or disposed of via certified shredding service.
- Document disposal actions in the Disposal Log (Appendix G).

8.4 Client Offboarding Procedure (Current + Required Documentation)

12. Confirm final deliverables provided to client via secure portal or encrypted method.
13. Export/compile client file package for the client (returns, key workpapers, final communications as appropriate).
14. Delete client data from active systems per the retention schedule and document deletion actions.
15. Provide the client with written confirmation of deletion (or what was retained and why).

System-specific offboarding steps (step-by-step)

A) Financial Cents (Portal, Messaging, Billing/Payments)

16. Close all open tasks/requests and confirm deliverables are complete.
17. Download/export the client’s deliverables package for the client (returns, PDFs, key documents) via the portal.
18. Provide the client their file package securely via the portal and confirm receipt.
19. Deactivate/archive the client in Financial Cents (remove portal access as appropriate).
20. Verify permissions: ensure only current team members retain access to the archived client record (least privilege).
21. Record actions taken (date, who, what exported/retained, confirmation sent) in the Offboarding Log.

B) TaxAct Professional (Return Data)

22. Confirm e-file acceptance and save acknowledgments with the client archive.
23. Generate final PDFs (return, signature forms, e-file authorization, and any required statements).
24. Move client’s TaxAct working data into your archived storage structure.
25. Remove any nonessential working copies (drafts, temp exports) from the workstation after archiving.
26. At the end of the 7-year retention period, delete the client return data using TaxAct’s deletion method and document completion.

C) Local Workstation (Encrypted Laptop)

27. Search and consolidate client files from common locations (Downloads, Desktop, scan folders, temp folders).
28. Move retained items into the encrypted 'Client Archives' folder with restricted access.
29. Securely delete non-retained items (empty recycle bin/trash; remove temp files).
30. Remove local copies from synced folders and verify deletion propagated.
31. Document completion in the Offboarding Log.

D) Backups (Backblaze B2)

32. Confirm the client archive location is included in encrypted backups.
33. Record the retention expiry date (7 years) for the client archive.
34. At retention expiry, delete the archived files from the source archive and allow backups to age out per backup retention/versioning policy.
35. Do not weaken immutability/retention lock controls; document deletions and expiry actions.
36. Record deletion/expiry in the Disposal Log.

E) Payments and Banking Records (Financial Cents + Novo)

37. Issue final invoice (if needed) and confirm it is paid/closed; export receipt for client.
38. Stop any recurring billing/authorizations tied to the client (if applicable).
39. Retain only accounting records needed for business/tax purposes for 7 years (no full card numbers stored locally).
40. Confirm no unusual payment/banking alerts occurred during offboarding; document any anomalies.

F) Client Confirmation

41. Send the client a confirmation message: deliverables provided, offboarding complete, and retention schedule (7 years) with deletion at end of retention.
42. If the client requests earlier deletion and no legal/business requirement to retain applies, perform secure deletion and send written confirmation of deletion.

9. Testing, Monitoring, and Program Adjustments

9.1 Safeguard Testing

- Monthly: verify device encryption is enabled; check endpoint protection status and last scan.
- Quarterly: review access lists and MFA status; review Financial Cents and TaxAct security settings.
- Quarterly: restore test from Backblaze B2 backup; document success/failure and corrective actions.
- Annually: risk assessment update and WISP review with documented sign-off.

9.2 Metrics and Evidence

- Maintain evidence for compliance: training logs, vendor review notes, access review checklists, incident logs, backup test logs.
- Store evidence in a secure internal folder with restricted access.

Appendices

Appendix A - Version History

Version	Date	Author	Summary of Changes
1.0	2026-01-01	Enoch Wright	Initial WISP created.

Appendix B - Asset Inventory (Template)

Maintain an up-to-date list of devices and critical accounts:

- Work laptop(s): make/model/serial, encryption status, OS version, assigned user.
- Mobile devices used for MFA: model, OS, screen lock enabled.
- Critical accounts: Financial Cents admin, TaxAct admin, Backblaze admin/API keys, Novo admin.

Appendix C - Access Review Checklist (Template)

- List all users and roles in Financial Cents; verify least privilege and active status.
- List all users and roles in TaxAct Professional; verify MFA enabled and active status.
- Review Backblaze B2 access keys/tokens; disable unused keys; rotate annually.
- Review Novo users and permissions; confirm 2FA and alerts.

Appendix D - Vendor Inventory

Vendor	Service	Data Involved	Security Evidence to Keep	Annual Review Date
Financial Cents	Client portal + practice management + billing	Client documents, messages, billing data	Security page, SOC attestation (if provided), MFA settings screenshots	
TaxAct Professional	Tax prep and e-file	Return data, transmissions	Security documentation, MFA settings, account admin list	
Backblaze B2	Encrypted backup storage	Encrypted backup archives	Encryption settings, key management notes, access key inventory	
Novo Bank	Business banking	Banking transactions	2FA/alerts settings, user list,	

account change logs

Appendix E - Training Log (Template)

Record training date, topics, attendee, and evidence (certificate/screenshot).

Appendix F - Incident & Alert Log (Template)

Record incident date/time, systems affected, actions taken, notifications, and closure summary.

Appendix G - Disposal Log and Media Sanitization Checklist (Template)

- Paper shredding date, method, and batch description.
- Device/media disposal: secure wipe method used; verification performed; disposition (recycled/destroyed).

Appendix H - References (Provider and Regulatory Resources)

Keep copies (PDF or screenshots) of key security documentation to support due diligence. Suggested sources include:

- FTC Safeguards Rule (16 CFR Part 314) and FTC business guidance on the Safeguards Rule.
- IRS Publication 5708 (WISP template) and IRS Publication 4557 (Safeguarding Taxpayer Data).
- Financial Cents Security page and portal security documentation.
- TaxAct Professional security documentation.
- Backblaze B2 encryption documentation (including server-side encryption options).
- Novo banking security and FDIC insurance documentation.

Operational Checklists

Checklist 1 — Client Offboarding (Per Client)

- □ Close all open tasks/requests; confirm deliverables completed.
- □ Provide client file package securely; confirm receipt.
- □ Financial Cents: deactivate/archive client; confirm portal access removed as appropriate.
- □ TaxAct: save acceptance proofs; archive final PDFs/records.
- □ Workstation: remove non-retained working copies; clear temp/download folders.
- □ Backups: confirm archive included; note retention expiry date (7 years).
- □ Payments: close invoices/recurring billing; retain only required accounting records.
- □ Send written confirmation to client (deliverables + retention/deletion info).
- □ Log offboarding actions (date, systems touched, staff initials).

Checklist 2 — Monthly Device & Security Hygiene

- □ Verify full-disk encryption enabled on work laptop(s).
- □ Run endpoint protection scan; confirm definitions updated.
- □ Install/verify OS and application updates.
- □ Review security alerts for Financial Cents, TaxAct, Backblaze, email, and banking.
- □ Confirm backups ran successfully; investigate any failures.
- □ Perform a restore test at least monthly during filing season; quarterly otherwise.

Checklist 3 — Quarterly Access & MFA Review

- □ Financial Cents: review users/roles; remove unnecessary permissions; confirm MFA enabled.
- □ TaxAct: review users; confirm MFA enabled; confirm admin recovery details controlled by QI.
- □ Backblaze: review users/API keys; disable unused keys; confirm MFA enabled on console accounts.
- □ Email accounts: confirm MFA enabled; review forwarding rules and connected apps.
- □ Novo: review users/permissions; confirm MFA/2FA and alerts enabled; verify contact info.
- □ Document completion (date, reviewer, notes).

Checklist 4 — Backup Restore Test Log

Date	Tester	Sample Data Restored	Restore Source (B2/Local)	Result (Pass/Fail)	Notes/Actions

Checklist 5 — Annual Vendor Security Review

- ☐ Confirm vendor list is current (Financial Cents, TaxAct, Backblaze, Novo, and any others).
- ☐ Collect security evidence (SOC report/attestation if available, security documentation, encryption/MFA details).
- ☐ Confirm contracts/terms include confidentiality and breach notification where feasible; document compensating controls if not.
- ☐ Review vendor admin settings (MFA, access logs, alerts).
- ☐ Record review date and findings; note follow-up actions.

Checklist 6 — Secure Disposal

- ☐ Electronic: use secure deletion/cryptographic erasure where available; confirm removal from active storage.
- ☐ Backups: ensure retention expiry + deletion/aging out is documented; do not weaken immutability settings.
- ☐ Paper: cross-cut shred or certified shredding; record date and batch description.
- ☐ Devices/media: wipe storage using a recognized method; verify wipe; record disposition.