



Coinfish Capital Advisors LLC

coinfishcapital.com · info@coinfishcapital.com

Written Information Security Program (WISP)

Coinfish Capital Advisors LLC

Version 2026-10 · Effective October 25, 2026. Prepared with reference to the FTC Safeguards Rule, 16 CFR Part 314 (as amended 2021 and 2023). This document is for general information and is not legal advice.

Firm	Coinfish Capital Advisors LLC (CCA), 160 Adams Avenue, Unit D PMB 1008, Hauppauge, NY 11788
Program owner / Qualified Individual	Mark O. Brazier, LL.B., EDFP, President and CEO
Scope	Client and guarantor information CCA receives for its advisory services: the Secure Client Portal (portal.coinfishcapital.com), email (info@coinfishcapital.com), the Qualified Individual's work laptop and phone, and paper records
Related documents	Portal Privacy Notice, Data Retention and Deletion Policy, Information Security Program Summary (NY SHIELD Act), Incident Response Plan (all version 2026-10-v1)

Does the Rule apply?

- CCA is a consulting firm. It is not a lender, broker, CPA or tax preparer.
- Where the Gramm-Leach-Bliley Act and the FTC Safeguards Rule apply to our services, this program is designed to align with the FTC Safeguards Rule.
- CCA maintains this program in all cases, because it handles sensitive client and guarantor financial data.

Small-entity exemption (314.6)

- Firms that keep customer information on **fewer than 5,000 consumers** are exempt from 314.4(b)(1) (written risk assessment), 314.4(d)(2) (pen tests and scans), 314.4(h) (written incident response plan) and 314.4(i) (annual report).
- CCA maintains **all four anyway** as good practice and rechecks the count each year.

(a) Qualified Individual — 314.4(a)

- **Mark O. Brazier, LL.B., EDFP, President and CEO** oversees, runs and enforces this program.
- No outside provider runs the program. If one is ever used, the Qualified Individual stays responsible and supervises it.

(b) Risk assessment — 314.4(b)

Data CCA holds

Data	Where it lives	Sensitivity
Business financials (P&L, balance sheet, debt schedule)	Portal (encrypted R2)	High
Business and personal tax returns	Portal	High
Bank statements	Portal	High
Guarantor personal financial statements and ID info inside documents	Portal	Very high
Contact details, intake answers, consents	Portal database (D1)	Medium
AI-assisted readiness memos	Portal database, Qualified Individual only	High
Website inquiries	Business email	Low-medium (kept up to 2 years)

The portal forms **reject SSNs and account/card numbers**. Uploaded documents may still contain them, so every document is treated as very high sensitivity.

Threats, likelihood and impact

Threat	Likelihood	Impact	Main controls
Phishing / stolen Google login	Medium	High	Google 2-Step, admin limited to one email, 1-hour admin session
Lost or stolen laptop/phone	Low-medium	High	Full-disk encryption, lock, remote wipe, no client files kept locally
Client sends documents by plain email	Medium	Medium	Portal is the required upload path; contact page says so
Web app bug / access-control flaw	Low	High	Automated tests (unit and integration), per-client folders, server-side checks
Encryption key loss	Low	High (files unreadable)	Offline backup under the Qualified Individual's control
Encryption key exposure	Low	Very high	Keys stored separately from data; never in code, logs or email
Vendor breach (Cloudflare, Google)	Low	High	Vendor review; object-level AES-256-GCM on top of vendor encryption
Insider / new staff misuse	Low (now)	High	Only the Qualified Individual has admin; onboarding training before any access
Ransomware on laptop	Low	Medium	No client files stored locally; portal is the system of record

- Reviewed **yearly** and after any major change (new system, new staff, new vendor, incident).

(c) Safeguards — 314.4(c)

- Access controls (c)(1)**
- Cloudflare Access protects the whole portal.
- Admin:** Google sign-in, limited to the Qualified Individual's account only, 1-hour session, plus a server-side email check.
- Clients:** one-time email PIN, 8-hour session; each client sees only their own folder.
- No shared logins. Access is removed the same day someone leaves.

6. **Data inventory (c)(2)** — the table in section (b); updated yearly.
7. **Encryption (c)(3)**
8. In transit: TLS/HTTPS with HSTS.
9. At rest: R2 storage encryption **plus** AES-256-GCM on every file. If the key is unavailable, uploads and downloads stop (fail closed). Keys are stored separately from data with an offline backup under the Qualified Individual's control.
10. Download links are signed, tied to the user and expire in 5 minutes. The storage bucket has no public URL.
11. **Secure development (c)(4)**
12. Strict security headers (CSP self-only, HSTS, no-referrer, frame-deny), file-type allowlist with content checks, 25 MB limit, rate limit of 30 requests per minute.
13. Full test suite must pass before every deploy.
14. **Multi-factor authentication (c)(5)**
15. Admin access requires Google 2-Step Verification.
16. Clients sign in with a one-time email PIN.
17. **Retention and disposal (c)(6)**
18. Files and personal details are deleted **90 days after an engagement is closed** by a daily job (09:00 UTC: 5 AM ET in summer, 4 AM ET in winter).
19. Clients can delete files any time or request full deletion (done within 30 days).
20. Website inquiries are kept up to 2 years.
21. Rule check: nothing is kept **more than 2 years after last use** unless a legal or business need requires it, or retention is not feasible. Legal holds are documented.
22. Disposal is logged. Devices are wiped before reuse or disposal.
23. **Change management (c)(7)**
24. Every change is tested locally, previewed, approved by the Qualified Individual, then deployed. Policy text carries a version number and date.
25. A backup copy is kept before each change.
26. **Monitoring user activity (c)(8)**
27. The audit log records every intake, upload, rejected upload, view, deletion, admin action, denied access and rate-limit block. It never holds document contents, AI prompts or memo text.
28. The Qualified Individual reviews the audit log **monthly**.

(d) Monitoring and testing — 314.4(d)

For a one-person firm, CCA uses periodic testing rather than continuous monitoring: - **Periodic** security testing of the portal, by a qualified outside tester or a documented self-test. - **Every 6 months** a vulnerability scan (web scanning plus a dependency audit of the code), and after any major change. - Monthly audit-log review and the automated test suite on every deploy.

(e) Training and staff — 314.4(e)

- The Qualified Individual completes yearly security and privacy training.
- **Onboarding:** anyone new gets training (phishing, document handling, the portal, reporting incidents) **before** any access. They acknowledge this WISP in writing.
- Staff get the least access they need. Only the Qualified Individual has admin access today.
- A training log (name, date, topic) is kept.

(f) Service providers — 314.4(f)

Provider	What it does	Oversight
Cloudflare	Hosting, sign-in (Access), encrypted storage (R2), database (D1), email routing	Yearly review of SOC 2 / ISO reports and data terms
Workers AI (Cloudflare)	Helps organize documents and prepare memos	Called directly; no AI Gateway , logging off; Cloudflare terms say content is not used to train models
Google (Workspace/Gmail)	Admin sign-in, business email	2-Step on; yearly review of security terms

- CCA chooses providers that can protect the data, requires safeguards through their contracts or terms of service, and reviews their security practices at least once a year.

(g) Keeping the program current — 314.4(g)

- Update this WISP after testing results, new systems, new staff, new vendors, any incident, or a change in business.
- Full review at least **yearly**.

(h) Incident response — 314.4(h)

- See the **Incident Response Plan** (v1): detect, contain within hours, assess, consult legal counsel, notify, fix, and review.
- Notify affected NY residents and regulators as the NY SHIELD Act requires.
- **FTC notification (314.4(j), effective May 13, 2024):** if unencrypted customer information of **500 or more consumers** is acquired without authorization, notify the FTC through its online form **as soon as possible and no later than 30 days** after discovery.

(i) Annual report — 314.4(i)

- CCA has no board. The Qualified Individual writes a **yearly review memo** to himself as sole member, covering program status, risk assessment, test results, incidents, vendor reviews and recommended changes. It is filed with this WISP.

Questions: info@coinfishcapital.com · Related policies at coinfishcapital.com.

The Coinfish Family of Businesses includes Coinfish Capital Advisors, Coinfish ATM Solutions, Coinfish Aviation, Coinfish Global Trade and Coinfish Farms. Each business operates independently.