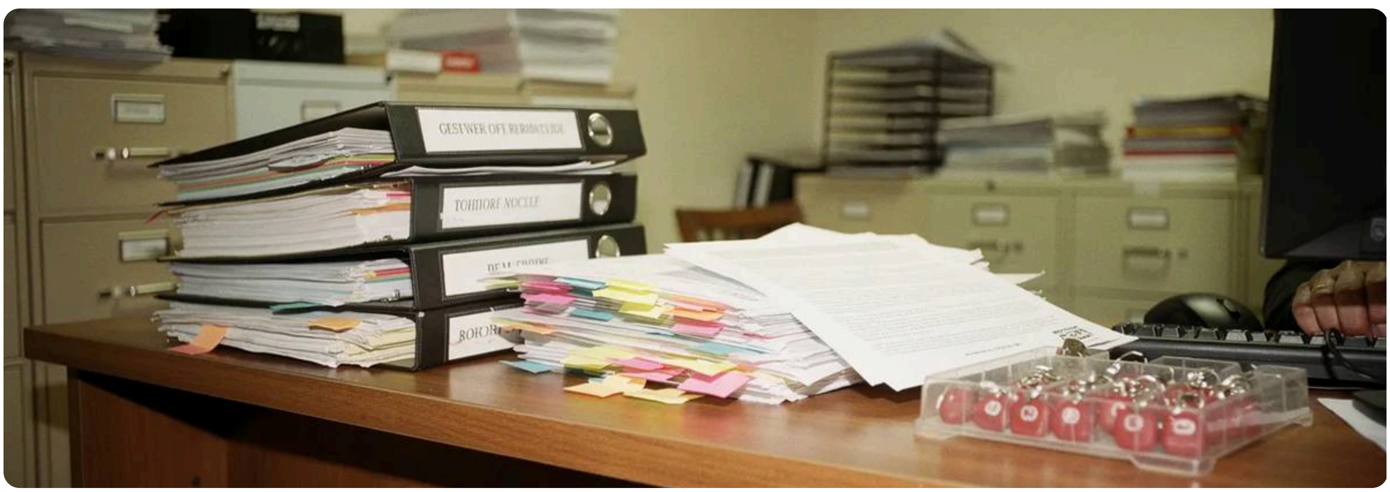
FUSION COMPUTING FIELD GUIDE

# Claude Cowork for real estate brokerages: secure deal files and FINTRAC-ready records for Canadian agents

**Mike Pearlstein, CISSP, MSc AI**

August 04, 2026



WHAT'S INSIDE

TRUSTED BY **Toronto law firms** **Hamilton manufacturers** **Vancouver clinics** **GTA accounting firms** **Ontario non-profits** **British Columbia professional services**

Brokers of record are asking whether Claude Cowork can clear the deal-file backlog without exposing client identification records. According to Statistics Canada, 12.2% of Canadian businesses now use AI, double the 6.1% of a year earlier, so someone in your office is already testing these tools. The duty to protect client information stays with the brokerage.

*Mike Pearlstein, CISSP, MSc AI, founder of Fusion Computing, which has secured IT for Canadian professional firms across Toronto, Hamilton, and Metro Vancouver since 2012.*

**Key takeaways**

- A brokerage can use Claude Cowork on a Team or Enterprise plan with access scoped to one transaction folder and a written policy.
- Deal-file assembly, listing copy, and offer summaries are strong fits. Client identification records and trust ledger data need tighter handling.
- Cowork stores its work locally, so it sits outside your audit logs. FINTRAC examinations and RECO inspections assume records you can produce, so you build that trail yourself.
- A registrant reviews anything that reaches a client. Never put deal files on a personal account.

**Plan a Safe Cowork Pilot**

## Can real estate brokerages use Claude Cowork with deal files?

Yes, a real estate brokerage can use Claude Cowork on a Team or Enterprise plan, with access scoped to one transaction folder and a written usage policy. According to the Trust in Real Estate Services Act and PIPEDA, the duty to protect client information binds the brokerage, not the software. On the business plans, your content is not used to train Anthropic's models by default, so deal files never belong on a personal account.

QUICK SELF-CHECK

### How AI-ready is your business, really?

Score your AI readiness across data, use cases, governance, people and ROI in about 2 minutes, with your ranked gaps and a 30/60/90-day plan.

**Take the AI readiness assessment →**

**or book a free 30-min call →**

Free · no email until you see your score, or talk to a senior engineer.

The point is that the obligations sit with the brokerage. RECO registers every agent and brokerage in Ontario and enforces conduct and record standards under TRESA, and no vendor setting moves that duty. What a brokerage controls is the scope: which folders the agent opens, which plan governs the data, and who reviews the work before a client sees it. On the business tiers, Anthropic's privacy commitments keep that data out of model training.

It's the same secure-adoption logic from the pillar guide on using Claude Cowork securely in your business, applied to a brokerage. The parallel guides cover law firms and accounting firms under their own regulators.

## What does Claude Cowork actually do for a brokerage?

> Claude Cowork completes multi-step office work rather than answering a single question. Per Anthropic's Cowork documentation, the agent works across your own files and apps on the desktop, so the practical jobs are deal-file assembly and checklists, listing descriptions and marketing copy, offer summary comparisons, commission statement prep, and organizing the paperwork behind FINTRAC records. Each output is a draft for a registrant to review.

Here's how those jobs map to the work, with the guardrail that keeps each one safe. Fusion Computing walks brokerages through this before any pilot, the same way we scope any AI services engagement.

**Book a 30-minute call to scope Claude Cowork for your brokerage safely →**

| Task | What Cowork does | The guardrail |
|---|---|---|
| Deal-file assembly | Builds transaction checklists and flags missing documents | Scope to one transaction folder; a registrant reviews |
| Listing copy and marketing | Drafts listing descriptions, feature sheets, and social posts | Facts checked against the listing agreement |
| Offer summaries | Compares competing offers into a plain-English table | Draft only; the agent presents, the client decides |
| Commission statements | Preps trade record summaries and month-end reconciliation drafts | Broker of record signs off; trust ledger stays out |
| FINTRAC paperwork | Organizes identification and receipt of funds records into the file | ID documents stay in the scoped folder, never a personal account |

## How do the confidentiality and FINTRAC guardrails work?

> According to Anthropic's deployment guidance, the core guardrail is least privilege: scope Cowork to one transaction's working folder, never the whole deal drive. Brokers and sales representatives keep client identification records, receipt of funds records, and large cash transaction records under FINTRAC's real estate obligations, and suspicious transaction reports are filed as soon as practicable. Cowork runs in an isolated virtual machine, but prompts still reach Anthropic, so scope limits exposure.

The mistake I flag most often is scope. When a brokerage connects the agent to the shared deal drive, a single task can read every client's identification documents going back years. Scope it to the active transaction and most of the risk disappears.

> **Field note.** A first-person field observation: in the office pilots I've run, the first thing I change is access. I've seen an admin point an agent at a drive holding every closed deal since 2019, ID scans included. We

> scoped it to one live transaction folder, and the workflow that felt reckless became routine. The work's identical; the exposure isn't.

The policy is the other half. A short rule set, the kind we cover in our guide on what belongs in an AI acceptable use policy, names the approved tool, the data that may go in, and who may run it. I pair the policy with a technical review so the scope survives a spring market.

Fusion Computing pairs that policy work with a cybersecurity review so the brokerage has a defensible position.

## The oversight gap for FINTRAC examinations and RECO inspections

> According to Anthropic, Claude Cowork stores its conversation history locally on each user's computer, outside audit logs, the Compliance API, and data exports. For a brokerage it matters: FINTRAC compliance examinations and RECO's record expectations both assume the brokerage can show how a record was produced and who touched it. Team and Enterprise owners can stream Cowork events to a SIEM through OpenTelemetry, which Anthropic notes does not replace audit logging for compliance.

According to Anthropic's guidance on using Cowork on Team and Enterprise plans, the local history "is not subject to Anthropic's standard data retention policies and cannot be centrally managed or exported by admins."

> **Field note.** When I walk a broker of record through the oversight gap, I open the local Cowork history on the demo machine and ask who else can see it. Nobody can. A FINTRAC examiner will ask how an

> identification record was compiled, and I have not yet met a brokerage whose compliance regime contemplated a transcript that lives on one admin's laptop.

> *"Brokers ask me whether Cowork can run the deal file. It can draft it. The trade record still belongs to the registrant who signs it, and the offices that hold that line get the speed without the compliance problem."*
>
> ***Mike Pearlstein**, CISSP, CEO, Fusion Computing*

That doesn't rule Cowork out. It means the brokerage designs its own record of AI-assisted work.

Fusion Computing wires the OpenTelemetry stream into the same monitoring we run for managed detection and response, so a brokerage sees tool calls and file access even though the transcript stays on the device. If a document could support a trade record or a FINTRAC filing, the office keeps that record on purpose.

## Plan tier and a setup checklist for a brokerage

> The plan tier is the first decision: per Anthropic's plan lineup, only Team ($25 USD monthly, $20 USD annual, 5-seat minimum) and Enterprise carry the "not trained on by default" commitment a brokerage needs. A safe rollout: scope to one transaction folder, keep "ask before acting" on for client files, write a usage policy, turn on OpenTelemetry monitoring, and keep a registrant reviewing anything a client sees.

Cowork runs on Pro, Max, Team, and Enterprise plans per Anthropic's release notes, but only the two business tiers fit client work. Here's the checklist Fusion Computing runs with an office before the first deal file goes near the tool. The steps come from our 2026 professional-firm pilots; in our practice the plan-tier fix is the first change we make.

**Why Canadian firms bring this work to Fusion Computing**

CISSP-led, a Microsoft Solutions Partner and a CompTIA Managed Services Trustmark holder, securing IT for Canadian SMBs across Toronto, Hamilton, and Metro Vancouver since 2012.

1. **Choose Team or Enterprise.** An agent running deal files on a personal account is the first risk to fix.
2. **Scope to one transaction folder.** Never the shared deal drive or the archive. Widen only with a reason.
3. **Default to “ask before acting.”** Cowork always asks before deleting files; keep approvals on for client data.
4. **Write an acceptable use policy.** Name the approved tool, the data that may go in, and who may run it.
5. **Turn on OpenTelemetry monitoring.** It’s the only visibility you have into what the agent did.
6. **Keep a registrant signing off.** Nothing client-facing, from offer summaries to trade records, ships without review.
7. **Map the terms to your duties.** Check Anthropic’s data handling against TRESA conduct rules and FINTRAC record-keeping before go-live.

None of it’s exotic, and most of it takes an afternoon.

Fusion Computing sets it up as part of the managed IT work we already do for professional offices, and the same pattern carries to wealth management firms and healthcare clinics under their own regulators. The review work is CISSP-led at a Microsoft Solutions Partner, the same team that has secured Canadian practices since 2012.

Claude Cowork is worth adopting for the deal-file and marketing work that fills a brokerage. The offices that set the plan, the scope, and the policy first are the ones that’ll use it calmly through a hot spring market while their competitors are still arguing about whether it’s allowed.

Fusion Computing helps Canadian businesses across Toronto and the GTA, Hamilton, and Metro Vancouver with managed IT, cybersecurity, and Microsoft 365.

## Frequently Asked Questions

### Q. Is Claude Cowork safe for deal files? –

Claude Cowork can be safe for deal files on a Team or Enterprise plan, with access scoped to one transaction folder and a registrant reviewing the output. The work runs locally and, on the business plans, is not used to train Anthropic's models by default. The duty to protect client information stays with the brokerage, so the controls around the tool are what make it safe.

### Q. Can Claude Cowork handle FINTRAC paperwork? –

Cowork can organize the documents behind FINTRAC records, such as sorting identification documents and receipt of funds paperwork into the deal file. The compliance obligation stays with the brokerage: a person verifies identity, signs records, and files any suspicious transaction report. Treat the agent as an assembler of the file, never the party that meets the obligation.

### Q. Does Claude Cowork breach client confidentiality under TRESA? –

Using Claude Cowork does not breach confidentiality by itself. The risk comes from careless setup. A brokerage should run Cowork on a business plan, scope it to one transaction folder, keep identification documents out of unscoped folders, and review anything before a client sees it. The conduct duty sits with the brokerage and its registrants, not the tool.

**Q. What plan does a brokerage need for Claude Cowork?** –

A brokerage should use the Team or Enterprise plan, not a personal Pro or Max account. Only the business tiers carry Anthropic's commitment not to train on your content by default, plus the owner and admin controls an office needs. An agent running client files on a personal account is the first risk to remediate.

**Q. Is client data used to train the model?** –

On Team and Enterprise plans, your content is not used to train Anthropic's models by default, so client information processed under a business plan stays out of training. Personal Pro and Max plans follow individual privacy settings, which differ from the business default. For a brokerage, that difference is the reason to standardise on a business plan.

**Q. How is Claude Cowork different from transaction management software?** –

Transaction management platforms are built around forms, signatures, and deal workflows. Claude Cowork is a general agent that works across your own files and apps on the desktop, so it drafts, compares, and organizes rather than managing signatures. Most offices use both: the platform remains the system of record, and Cowork does the reading and drafting around it.

**Q. Does Claude Cowork work on Windows or only Mac?** –

Claude Cowork works on both macOS and Windows through the Claude desktop app, and it reached general availability on both on April 9, 2026. It is not available on the web or on mobile. Some capabilities, such as computer use, arrived first as research previews, so confirm the current feature list for your platform inside the app.

**Q. Who at the brokerage should run Claude Cowork?** –

Start with a small group who understand the deal file and the confidentiality duty, not every agent at once. Cowork is an organization-wide setting that owners can switch on or off, and granular per-user controls are limited, so a deliberate pilot with named users beats a broad rollout. Pair it with training and a written policy before wider use.

**Talk to Fusion**

## Put this guide to work

Fusion Computing helps Canadian SMBs adopt AI safely. The review work is CISSP-led at a Microsoft Solutions Partner and CompTIA Managed Services Trustmark holder, securing Canadian businesses since 2012.

- Managed IT support with a 1-hour priority response
- Cybersecurity, managed detection and response, and compliance reviews
- AI and Copilot consulting, including safe Claude Cowork pilots
- Microsoft 365 management and licensing

**Book a 30-minute scoping call**

fusioncomputing.ca/contact-us · 416-566-2845
Toronto · Hamilton · Metro Vancouver