

Claude Cowork for construction firms: secure bid, contract, and project document work

Mike Pearlstein, CISSP, MSc Computer Science (AI)

Published May 27, 2026; Updated August 12, 2026



WHAT'S INSIDE

1. Can construction firms use Claude Cowork on bids and contracts?
2. What does Claude Cowork actually do on a construction project, explained
3. The bid-confidentiality and contract-data guardrails
4. What the Construction Act prompt-payment clock requires of your paperwork
5. The oversight gap for contract records and audits
6. Cowork versus the AI already inside your estimating software
7. How much does Claude Cowork cost a construction firm?

8. Plan tier and a setup checklist for a construction firm

9. Where a construction firm should start this week

10. Frequently Asked Questions

fusioncomputing.ca · 416-566-2845 · CISSP-led managed IT, cybersecurity, and AI for Canadian SMBs · Toronto · Hamilton ·
Metro Vancouver



TRUSTED BY

Toronto law firms Hamilton manufacturers

Vancouver clinics GTA accounting firms Ontario non-profits

British Columbia professional services.

Construction firms want to know whether Claude Cowork can take the document load off a bid or a project without leaking competitive pricing or a client contract. According to **Statistics Canada** (2026), 9.2% of Canadian construction businesses used AI in the 12 months to the second quarter of 2026, against 19.2% across all industries. The duty to protect bid and contract confidentiality stays with the firm.

Mike Pearlstein, CISSP, MSc Computer Science (AI), founder of Fusion Computing, which has secured IT for Canadian construction firms across Toronto, Hamilton, and Metro Vancouver since 2012.

The estimators getting real value from AI scope it to 1 bid folder and keep margins out of the prompt. Confidentiality discipline is what makes it safe to use on a live job, and it is the only control that survives a busy tender week.

Mike Pearlstein, CISSP, founder of Fusion Computing.

Key takeaways.

Book a Consultation

- Claude Team runs from 2 to 150 members at US\$20 per seat per month billed annually, so 1 estimator and 1 PM can pilot without a firm-wide purchase.
- Scope Cowork to 1 bid or project folder, never the whole tender archive.
- Local sessions sit outside your audit trail. Cowork run through web and mobile is captured in the Compliance API, and on Enterprise that cloud mode is off until an owner turns it on.
- The Construction Act gives an owner 28 days to pay a proper invoice and only 14 days to dispute it, so paperwork errors cost money fast.
- A person reviews anything submitted to an owner or a subcontractor. Interest under s.6.9 runs automatically on late payment.

Can construction firms use Claude Cowork on bids and contracts?

Yes, on a Team or Enterprise plan. According to [Anthropic's commercial terms](#) (2026), "Anthropic may not train models on Customer Content from Services". Your duty to keep competitive pricing and contracts confidential survives that promise, so scope the agent to 1 bid folder first.

The control that matters is scope: which files the agent opens, which plan governs the data, and who reviews the output before it goes to an owner or a sub. Bid confidentiality depends on keeping the numbers controlled, so the setup around the tool is what keeps it safe.

This spoke applies the secure-adoption logic from the pillar guide on [using Claude Cowork securely in your business](#) to a contractor, and it sits alongside our broader [IT for construction firms](#) work.

The design consultants on your projects face the same clocks from the other side, which the companion [Claude Cowork guide for architecture and engineering firms](#) covers.

AI use by Canadian businesses, Q2 2026.

Share reporting AI use in producing goods or delivering services.

All industries.

19.2%

Construction.

9.2%

Source: Statistics Canada, table 33-10-1167-01, Canadian Survey on Business Conditions.

What does Claude Cowork actually do on a construction project, explained

It finishes multi-step document work. According to [Anthropic's release notes](#) (2026), Cowork reached general availability on macOS and Windows on April 9, 2026, then gained web and mobile access on July 7, 2026. For a contractor that means tenders, RFIs, contracts, safety files, and billing drafts.

Here's how those 5 jobs map to the work, with the guardrail that protects the firm. Fusion Computing walks contractors 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 firm safely →](#)

Task	What to test	The guardrail that keeps it safe.
Bid and tender assembly	Pulls a tender package together from your templates and docs	Scope to 1 bid; an estimator verifies.
RFI and change-order drafting	Drafts RFIs and change orders from project records	Project data stays in the scoped folder.
Contract and subcontract organization	Sorts and renames contracts, POs, and records	1 project folder, never the tender archive.
Safety and COR document prep	Organizes safety and certification documents	Internal documents, reviewed before filing.
Progress billing and lien drafts	Assembles progress-billing and lien-notice drafts	A draft for review, checked before serving.

Treat these as pilot hypotheses to validate in your own tenant, not vendor-guaranteed capabilities. Anthropic documents a subset of them directly; the rest are workflows to test before a firm relies on them.

The bid-confidentiality and contract-data guardrails

Least privilege is the whole control. According to **Anthropic's safety guidance** (2026), prompt-injection risk stays “non-zero” even with classifiers running. The folder you point the agent at is the real boundary, so scope it to the active job rather than the tender archive.

The first thing I check is scope. When a firm points the agent at the whole tender archive, 1 task can read every bid and price. Scope it to the active job and you have cut most of the risk.

FIELD NOTE FROM MIKE. The first thing I change is access. I've watched an estimator point an agent at a drive holding every open and closed bid. We scoped it to 1 job folder, and the workflow that felt reckless became routine. The work's identical; the exposure isn't.

What may go in, and what must not.

- **In:** working documents for the 1 active job, RFIs, and drafts of your own correspondence.
- **Out:** competitive pricing and subcontractor quotes for any job outside that folder.
- **Out:** the tender archive, the full contract library, and shared network drives.
- **Always:** a person on anything submitted to an owner, a consultant, or a subcontractor.

Anthropic documents 3 approval modes, and the one a contractor wants is Manually approve. Deletion is protected in every mode, since Cowork “requires your explicit permission before permanently deleting any files”. Treat that as a floor rather than a scoping control.

The policy is the other half. A short rule set names the approved tool, the data that may go in, and who may run it, and I keep it to 1 page for a contractor. We cover the shape of it in our guide on [what belongs in an AI acceptable use policy](#), paired with a [cybersecurity](#) review so the firm protects its margins.

What the Construction Act prompt-payment clock requires of your paperwork

The clocks are short. According to the Ontario [Construction Act](#) (2026), s.6.4(1) obliges an owner to pay a proper invoice within 28 days. Section 6.4(2) leaves the owner only 14 days to give a notice of non-payment, and s.6.5(1) gives you 7 days to pay your subcontractors.

REGULATOR QUOTE. Section 6.9 says interest “begins to accrue on an amount that is not paid when it is due to be paid under this Part”. The rate is the prejudgment rate under s.127(2) of the Courts of Justice

Act, or a higher contract rate. Nobody has to claim it. The 2024, c. 20, Sched. 4 amendments came into force on January 1, 2026.

That reframes the AI question. An agent drafting an invoice, a notice, or a change order is working inside a statutory clock measured in days, with interest running and interim adjudication under Part II.1 available to the other side.

Why a proper invoice is the thing to get right.

Section 6.1(1) lists what a written bill must contain before it counts as a proper invoice, from the contractor name and address to the contract identifier and the payment period. Miss an item and the 28-day clock may never start. In our practice that is the single most useful thing to hand an agent, because it is a checklist rather than a judgement call.

CONTRARIAN THESIS. Construction is near the bottom of Canadian AI adoption at 9.2%, and the usual reading is that the sector is behind. I read it differently. The document work that pays here is invoicing, notices, and RFIs, all of which sit on statutory deadlines. A slow start is a rational response to a fast clock rather than a technology gap.

The oversight gap for contract records and audits

Where the session runs decides the record. According to [Anthropic's admin guidance](#) (2026), local session history stays on the user's computer and "cannot be centrally managed or exported by admins". Cowork via mobile and web is captured in the Compliance API instead.

That split is the setting I check first on any contractor engagement. Cloud sessions are on by default for Team plans and off by default for Enterprise, where an owner switches them on and grants the capability through custom roles.

Where the record actually lives.

- **Local session:** history sits on the laptop, outside admin export and outside the Compliance API.
- **Web or mobile session:** runs on Anthropic infrastructure and is captured in the Compliance API.
- **OpenTelemetry stream:** tool calls and file access, in your own monitoring, for either mode.

The Enterprise **audit logs** capture metadata rather than the work itself. Owners can also stream Cowork events to a SIEM through OpenTelemetry, which Anthropic notes “doesn’t replace audit logging for compliance purposes” on its own. Cowork exports the full text of user prompts by default, along with tool parameters, file paths and user email addresses, so configure filtering or redaction at the collector and set SIEM access and retention before enabling export. Our engineers found that stream is where tool calls and file access become visible.

If the pilot needs centralized monitoring, define the destination, filtering, access and retention before enabling OpenTelemetry.

Cowork versus the AI already inside your estimating software

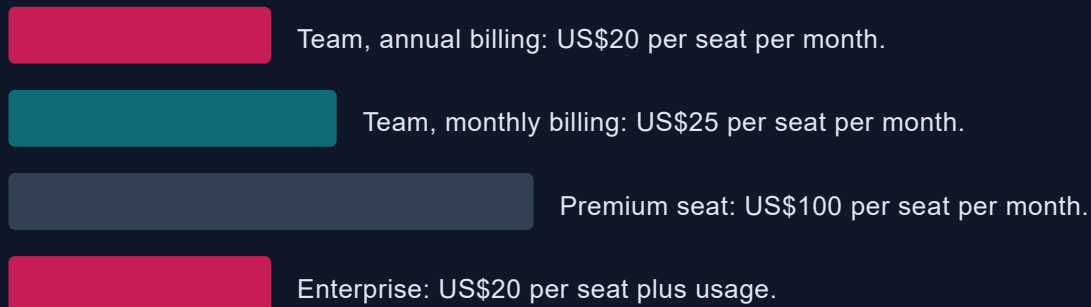
Blast radius is the difference. Construction-platform AI is embedded in an estimating, project-management, or accounting system and scoped to that system’s data. Claude Cowork reaches across your own files instead, so a takeoff model sees 1 dataset while a desktop agent sees whatever folder and connectors an owner granted it.

That difference cuts both ways, and the question I ask first is which system already hands you an audit trail. A project-management vendor usually carries part of that burden for you. With Cowork the firm owns the scoping decision, so the upside is that the agent works on the odd, cross-system documents no platform ever covered.

How much does Claude Cowork cost a construction firm?

Less than the scoping work around it. According to Anthropic's published pricing (2026), Claude Team is built for 2 to 150 members at US\$20 per seat per month billed annually, or US\$25 billed monthly. A premium seat with 5 times the usage is US\$100. Enterprise is US\$20 per seat plus usage at API rates.

Claude plan pricing, 2026 (US dollars).



Team	Team, annual billing: US\$20 per seat per month.
Team	Team, monthly billing: US\$25 per seat per month.
Premium seat	Premium seat: US\$100 per seat per month.
Enterprise	Enterprise: US\$20 per seat plus usage.

Two numbers matter when I size this for a contractor. The floor is 2 licences, so 1 estimator and 1 project manager can pilot without a firm-wide purchase. The ceiling is 150 people, above which the plan is Enterprise.

In our practice the licence is rarely the expensive part. We measured the real cost sitting in scoping, policy drafting, and the monitoring wiring, at 3 to 6 hours for a Hamilton contractor rather than a per-seat charge.

Plan tier and a setup checklist for a construction firm

Plan tier is the first decision. According to [Anthropic's privacy centre](#) (2026), an individual plan with the improvement setting enabled may keep chats “in a de-identified format for up to 5 years in our model training pipelines”. Business inputs and outputs are deleted within 30 days by default.

Need the policy first? Use our [AI acceptable use policy template](#).

That 5-year gap is the whole argument for buying 2 seats, because only Team and Enterprise carry the contractual no-training commitment plus the admin controls a firm needs.

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.

[Get a CISSP-led review of where AI tools touch your bids and contracts →](#)

The 8-step rollout.

1. **Choose Team or Enterprise.** Competitive pricing on a personal account is the first risk to fix.
2. **Scope to 1 bid or project folder.** Never the whole tender archive. Widen only with a reason.
3. **Set the approval mode to Manually approve.** Deletion always prompts, and pricing should too.
4. **Decide the cloud-session question.** Team has it on by default; Enterprise owners must switch it on deliberately.
5. **Write an acceptable use policy.** Name the approved tool, the data that may go in, and who may run it.

6. **Turn on OpenTelemetry monitoring only after deciding what may be logged.** On local sessions it's an additional visibility stream into what the agent did.
7. **Keep a person signing off.** Nothing submitted to an owner or a sub ships without review.
8. **Check every invoice against s.6.1(1).** A bill that is not a proper invoice may never start the 28-day clock.

FIELD NOTE FROM MIKE. I ask 1 question before any of the 8 steps above: who reviews this document today, when a human writes it? If nobody at the firm can name that person, the AI pilot is not the problem I want to solve first. Cowork simply makes an informal review step visible sooner than an owner's consultant would.

None of it's exotic. The technical setup can be quick; the privacy, logging and approval work is what decides how long the pilot takes. Fusion Computing sets it up as part of the **managed IT** work we already do for firms across **Toronto and the GTA**. The same pattern carries to **manufacturers** under their own rules.

Where a construction firm should start this week

Buy 2 Team seats and scope them to 1 live job folder. Set approvals to Manually approve, and put the cloud-session decision in writing before anyone opens a second folder. Fusion Computing runs that scoping session in an afternoon. If you want a CISSP-led second opinion first, **talk to us** or read more **about how we work**.

Related construction IT guides.

- **Cybersecurity for construction firms in Canada**

Frequently Asked Questions

Q. Is Claude Cowork safe for competitive bids? —

Claude Cowork can be safe for bid work on a Team or Enterprise plan, with access scoped to 1 bid folder and an estimator reviewing the output. Team and Enterprise do not train on organization content by default, but that alone is not a confidentiality determination: verify the execution mode, Anthropic's current terms and DPA, retention, the applicable privacy law and your professional obligations before client data is used. Anthropic's commercial terms say it may not train models on Customer Content, and business inputs and outputs are deleted within 30 days by default. Expose only the documents a task needs.

Q. Can Claude Cowork assemble tender documents? —

Yes. Cowork can pull a tender package together from your templates, specs, and past submissions, which saves an estimating team hours. Treat the assembled package as a draft for a person to verify, and keep it in a scoped bid folder so the agent sees only the 1 active job rather than the whole tender archive.

Q. Can AI drafting break the prompt-payment clock? —

It can, and the failure is quiet. The Construction Act starts the 28-day payment clock from a proper invoice, and s.6.1(1) lists what that bill must contain. An agent that drops the contract identifier or the payment period produces a document that may never start the clock. Keep a person checking every invoice against the statutory list before it is issued.

Q. What plan does a construction firm need for Claude Cowork? —

Team or Enterprise, never a personal Pro or Max account. Claude Team runs from 2 to 150 members at US\$20 per seat per month billed annually. Above that ceiling, or where you need groups and custom roles to enable Cowork for estimating only, the answer is Enterprise. Competitive pricing on a consumer account is the first risk our CISSP-led review looks for.

Want an AI use policy that protects your competitive pricing? →

Q. How is Claude Cowork different from construction software AI? —

Construction software AI is usually built into estimating, project-management, or accounting platforms and scoped to those systems. Claude Cowork is a general agent that works across your own files and apps, which suits document and bid work more than scheduling or takeoff. The practical difference is blast radius: a takeoff model sees 1 dataset, while an agent sees whatever folder you granted it.

Q. Does Claude Cowork help with safety paperwork? —

Yes. Cowork can draft and organize safety policies, COR documentation, and toolbox-talk records from your own materials. Treat the output as a draft for a safety lead to review, and keep a record of how it was produced. A local Cowork session history stays on the laptop and is not captured in central audit logs or the Compliance API.

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

—

Both, and on more surfaces since launch. Cowork reached general availability on macOS and Windows through the Claude desktop app on April 9, 2026. On July 7, 2026 Anthropic added web at claude.ai and the Claude mobile apps, in beta for Team and Enterprise, with those sessions running on Anthropic's infrastructure rather than the laptop. Confirm the current feature list inside the app.

Q. Who at the firm should run Claude Cowork?

—

Start with a small group of estimators or project managers who understand bid confidentiality, never the whole firm. The Cowork toggle is organization-wide, so a Team plan is all-or-nothing. On Enterprise, groups and custom roles let an admin enable Cowork, or the cloud-session capability, for named teams only. Pair whichever you choose with training and the written policy Mike Pearlstein reviews before a pilot.

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