MARKORA

SECURITY & DATA HANDLING

How Markora handles your firm's access and *data.*

Professional services firms hold other people's confidential information. This is how Markora works with it — the short version for partners, with the detail on page 2 for whoever handles IT and risk.

01

Your data stays in your accounts

Everything is built and configured inside the firm's own Microsoft 365, Google Workspace, CRM and practice-management accounts. Client information never passes through or is stored in Markora systems.

02

Least access, for the shortest time

Markora works through a named account or delegated access that the firm creates and controls — never a shared password — with only the permissions the build needs. It is removed at hand-over.

03

No training on your data

AI tools are set up on business plans whose terms exclude using the firm's data to train models. This is checked for every tool, on every engagement, before any client data is involved.

04

A professional stays in the loop

Anything that reaches a client is reviewed and approved by a person at the firm. Agents do not act on client matters without a human approval step.

05

Designed around your obligations

Workflows are designed around PIPEDA and the firm's regulator — Law Society of Ontario, CPA Ontario, CIRO or others — from the first session. If something can't be done safely, Markora says so.

06

Everything handed over

At completion the firm receives full documentation, all credentials it doesn't already hold, and confirmation that Markora's access has been removed.

QUESTIONNAIRES

Happy to complete *yours*

If the firm has its own vendor security questionnaire or data-processing terms, Markora will complete or sign them before any access is granted. A confidentiality agreement is available on request.

CONTROLS

AREA	WHAT MARKORA DOES
Access to firm systems	Named or delegated account created by the firm; role-based permissions limited to the build; multi-factor authentication required; no shared passwords.
Access removal	All Markora access removed within one business day of hand-over, confirmed to the firm in writing. The firm can revoke access at any time.
Markora's own accounts	Unique passwords held in a password manager; multi-factor authentication on email, cloud and every admin account.
Devices	A dedicated work laptop with full-disk encryption, automatic OS and security updates, screen lock and endpoint protection. No client work on shared or personal devices.
Client data	Stays in the firm's systems. Not downloaded, emailed or copied to Markora storage. Test data is anonymised or synthetic where possible.
AI tools	Business or enterprise plans only, with terms that exclude training on customer data; data-retention settings reviewed per tool; no client data in personal or free-tier AI accounts.
Measurement data	Time logs stay in the firm's systems and are reported by role. Any copies are returned or deleted at the end of the engagement.
Incidents	Markora tells the firm within 24 hours of becoming aware of any incident affecting its data or access, and helps it meet its PIPEDA breach-reporting obligations.
Documentation	Every build is documented: what was configured, where data flows, who has access, and how to switch it off.
Insurance	[Professional liability and cyber insurance: insurer and limits — add once bound. Certificates available on request.]

WHAT WE ASK OF THE FIRM

- → Create Markora's access in your own systems, with the permissions agreed in the proposal
- → Tell us about any policy, regulator guidance or client commitment that applies
- → Nominate a person to approve client-facing outputs and agent actions
- → Confirm at hand-over that access has been removed

WHO IS RESPONSIBLE FOR WHAT

- → The firm owns its data and its clients' data, and decides how it is used
- → Markora acts on the firm's instructions, within the access the firm grants
- → The firm's IT provider keeps responsibility for infrastructure and security settings; Markora works alongside them

CONTACT

Markora is the operating name of Markora AI Solutions Inc. Security or privacy questions: hello@markora.ai. Our privacy policy is at markora.ai/privacy.html. This statement describes how Markora works; the proposal and any signed agreement set out the binding terms.