AI at Scratchpad, Inc.

Scratchpad and Clearskies are both products of Scratchpad, Inc., built and operated under the same security standards and covered by a single SOC 2 Type II certification. The following covers how we use AI across both products — what it does, what data it accesses, and how that access is controlled. Where the two products differ, we've noted it.

Do you train AI models on our data?

No. We don't train on customer data, and our LLM sub-processors are contractually prohibited from doing so either.

What does your AI do?

- **Generates content** — summaries, briefs, drafts, and collateral from real customer interactions
- **Surfaces context** — CRM data, call highlights, emails, and deal history when your team needs it
- **Updates your CRM** — where configured, agents write call summaries, next steps, and activity logs back to Salesforce

Clearskies connects as an MCP server to Claude, ChatGPT, or any AI — giving it live access to a unified context graph of your CRM, calls, email, calendar, and Slack. Teams use it to build agents and run cross-system queries directly inside the tools they already use.

How is access controlled?

The AI can only access data the authenticated user is already authorized to see.

Scratchpad inherits each user's Salesforce API permissions. Your rules, guardrails, and field-level restrictions apply automatically.

Clearskies access flows from the integrator's authorization scope. The integrator controls which sources are connected and how access is scoped.

All customer data is logically isolated. No customer can access another's data.

What data does your AI have access to?

Your admin configures what data we have access to. Nothing is ingested without explicit authorization.

Scratchpad: limited to what each user can already access via their Salesforce permissions.

Clearskies: the admin determines what sources are connected and what gets ingested.

Depending on your configuration, connected sources include:

- CRM data
- Call recordings and transcripts
- Email and calendar data
- Messaging platforms (e.g. Slack)

New connectors are added regularly.

What can agents do — and what can't they?

Agents can:

- Query connected data to answer questions and generate outputs
- Take actions within connected systems where configured
- Surface results via Slack, the agent builder, or MCP server

Agents cannot:

- Access data from sources the customer has not connected
- Act beyond the authenticated user's permission boundary
- Access or affect any other customer's data
- Access or modify underlying systems or databases directly

Who are your LLM sub-processors?

We partner with leading LLM providers. Key commitments:

- Providers are contractually prohibited from using customer data to train or improve their models
- Customer data is treated as confidential
- Refer to our sub-processor list and DPA for current providers and full contractual detail