

Miro AI Workflows: AI Security



Product Overview

Think of Miro as a shared canvas where teams plan, create, and align in one place. With Miro AI Workflows, your "workflow" is simply how your team moves from messy inputs to finished outputs—on the same canvas—using three building blocks: **Miro Flows**, **Miro Sidekicks**, and **Knowledge**.

Miro Flows are visual, multi-step AI automations you build right on the canvas: you connect existing board content/widgets and AI instructions to automatically turn work into outputs like docs, tables, slides, or prototypes. Users can save and reuse the process as a template. Flows can also plug into enterprise knowledge sources and let you pick the AI model best suited for the task, so the results reflect your company's context.

Miro Sidekicks are conversational AI teammates that collaborate with you on the shared canvas. You can choose a pre-built Sidekick or create your own; they read selected on-canvas context so you don't need elaborate prompts, and they help you produce the right format for the moment—whether that's a summary doc, a diagram, or slides. Sidekicks can be equipped with your organization's knowledge and support model selection, so their guidance and outputs align with your standards.

Knowledge connects Miro to enterprise providers like Glean, Amazon Q (Beta), Gemini Enterprise (Beta), Microsoft Copilot (Beta), and Miro Insights, so teams can pull trusted, current information onto the canvas and use it as context for Sidekicks and Flows. You can invoke Knowledge from Sidekicks, inside Flows (for AI instructions or doc editing), or through a standalone chat, before converting what you find into docs, tables, sticky notes, or slides. Admins define which integrations are enabled and who can use them.

USER DATAFLOW

Sidekicks

The Miro Sidekicks dataflow begins with the user choosing their Sidekick on the canvas and sending their prompt input and board context to the Sidekicks API gateway, which routes to the Sidekicks Service orchestrator.

This service first undergoes a check with the Compliance and Governance services before proceeding to context assembly and prompt construction. The workflow then invokes the LLM of choice via a model gateway that enforces guardrails. The final outputs undergo validation, are normalized, and streamed back to the client.

The Sidekicks service uniquely maintains persistent application data for conversation history (where our other features are stateless), though LLM input/output logging is opt-in.

Flows

The Miro Flows feature starts when a user triggers a flow to run within the canvas, which first checks authorization and settings within the Compliance and Governance Services. The AI Gateway selects the correct process and immediately applies essential compliance filtering (like checking for sensitive prompts) via our Core AI service.

The request is then routed to the LLM of choice through a gateway, which can use optional tools such as our Knowledge or Sidekicks features. The process is able to manage complex, multi-step tasks and is designed to be largely stateless regarding customer data.

Like Sidekicks, the separate Flow service consults the AI compliance service and the AI model gateway for LLM interaction. After internal checks, and transforming the output, the final response is delivered back to the client.

Knowledge

The Knowledge feature dataflow kicks off with a user query in the Miro AI Panel, validated and audited by the AI Gateway, followed by safety filtering from the AI Compliance and Governance Services.

A routing agent directs the request to the Knowledge Gateway, which retrieves context from enterprise and external sources (like Glean, Copilot, or Amazon Q). The Knowledge service manages these external integrations by using the individual user's ID for access control and permissions.

The retrieved context relies on moderation from its trusted source. When it is sent back to Miro it is then transformed as output that is returned to the client in the chat or on the canvas.

ADDITIONAL SECURITY CONTROLS

Administrators can enable or disable Sidekicks and Flows on a team by team basis.

If a feature, such as document editing, image generation, or slide creation, wouldn't normally be available to the user, it's automatically unavailable to their Sidekick or Flow as well.



Sidekicks

Specific teams (3)

Custom AI partners that collaborate on exploring ideas, building solutions, and moving work forward.

[Learn about Sidekicks](#)

- ☒ **Restrict sharing of company Sidekicks**
Only admins with content management privileges can share company Sidekicks with everyone in the organization.
- ☒ **Restrict publishing to Miroverse**
Only admins with content management privileges can publish Sidekicks to Miroverse.
- ☒ **Restrict use of community Sidekicks from Miroverse**
Users can only use Sidekicks created by Miro or your organization.



Restricted capabilities in Sidekicks

Some features are not available to everyone in your organization. Manage access in **Images**.

ADDITIONAL SECURITY CONTROLS, continued

AI provider management

At the company level, administrators can define which AI providers are available for use, enabling or disabling them as needed.

Capabilities

Features

AI models

Available AI models

For some features, users can select the AI model they want to use. Manage which AI providers and models will be available for them to choose from. [Learn about AI model selection](#)

Docs

Create and edit documents with AI

Anthropic

Hosted on Amazon Bedrock

Google

Hosted on Google

OpenAI

Hosted on Azure OpenAI

Images

Generating images with AI in Miro. Does not include images that are part of Slides or Prototypes.

Amazon Bedrock

Hosted on Amazon Bedrock

Google

Hosted on Google

Stability AI

Hosted on Amazon Bedrock

Model selection in Flows

When using Flows, users can [select](#) which model they prefer to use from the models that have been approved for use.

A full and up to date list of the models used by Miro, as well as what they're used for, can be found [here](#).

Generate a Flow instruction

Run

Write a prompt to generate AI instructions

Amazon Bedrock

Claude 3.7 Sonnet

Claude 4 Sonnet

Claude 4.5 Sonnet Recommended

Sidekick sharing

Administrators can define whether users can share or publish their Sidekicks with the rest of the company, or the Miroverse marketplace.

Similarly, they can restrict users from importing Sidekicks from the Miroverse to use on their boards.

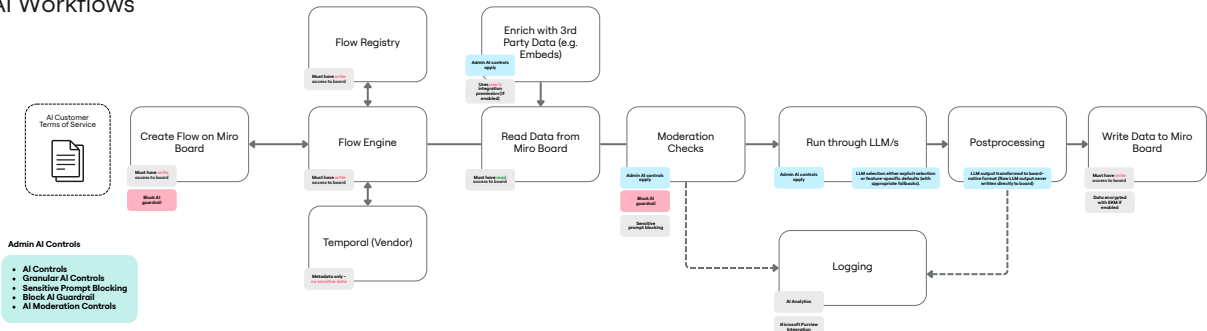
- ☐ Restrict sharing of company Sidekicks
Only admins with content management privileges can share company Sidekicks with everyone in the organization.
- ☐ Restrict publishing to Miroverse
Only admins with content management privileges can publish Sidekicks to Miroverse.
- ☐ Restrict use of community Sidekicks from Miroverse
Users can only use Sidekicks created by Miro or your organization.

MIRO AI FEATURE COMPARISON

	Foundational Security Controls (ISO 42001, Miro Architecture Level)	AI moderation levels (Strict, Default, Minimal)	Global AI access controls by capability (Everyone/No one/Specific teams)	View models used by each AI feature	Access controls for Flows and Sidekicks (Workflows SRLL) Everyone/No one/Specific teams	Admin Analytics (Overview + Miro AI dashboards)	AI Provider Management (OpenAI, Anthropic, Google)	Feature-level controls for individual AI features (granular toggles inside a capability)	Intelligent Guardrails: block Miro AI usage on classified boards	Prompt blocking in g. detect/source-code or sensitive terms; block at submission	AI Custom Terms of Service	Microsoft Purview DSPM for AI (forward prompts/responses for centralized governance)	AI Interaction Logs (prompt/response capture; API access and integration point)
Miro Enterprise + Workflows	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗

DATAFLOW DIAGRAMS

AI Workflows



Sidekicks

