Cumulus AI™

Download on the App Store

GET IT ON Google Play

Frequently Asked Questions: Cumulus AI Security

What is the source of the data used by Cumulus AI?

Cumulus AI leverages an API to communicate with OpenAI's GPT 3.5 LLM (large language model). The procedure document or prompt input by the user is the main source used to create your workflow. This LLM is pre-trained with a broad range of content, but it does not have access to a professional library or web searches. The generated workflow might not take into account details from other documents referenced in your input, such as engineering or construction codes. You can edit the generated workflow to be sure that any of these details are properly included.

What happens to my data when I upload it into Cumulus AI? Is it secure?

Data uploaded into Cumulus AI is NOT used to augment ChatGPT or further train the LLM. Note that OpenAI, ChatGPT's parent company, retains data for up to 30 days to help flag abuse. For more information, view Open AI's privacy policy.

Cumulus treats all data as confidential and securely stores your data in the cloud. All your data is always encrypted, whether it is in-flight or at rest. Our information retention policy governs how we handle all types of data, which you can read more about in our terms of service and privacy policy.

How does Cumulus AI ensure that prompts are secure?

You may have heard of indirect prompt injection, which is an LLM security flaw that users of Generative AI technology are always concerned with. This occurs when a user prompts the LLM in a way to cause it to inject malware.

Cumulus AI mitigates this risk, because our software was built with an intermediary so that users are not prompting the LLM directly as with a chat box. Instead, our system uses an API to communicate with the LLM and seeds the prompt with a specific schema so that it responds with outputs in a consistent format. This protects our users from indirect prompt injection.

Cumulus AI™

How do I know that workflows generated by Cumulus AI are accurate?

We consider our users as the subject matter expert on their procedures. By using Cumulus AI, you agree to the following terms and conditions: "The user is responsible for verifying that the workflow and other information generated using Cumulus AI is appropriate for accomplishing the intended task. Cumulus is not responsible for the actions that are performed using the workflow generated with the app. Cumulus prohibits the use of Cumulus AI for harmful and illegal activities."

Our shared responsibility model specifies that it is ultimately the user's responsibility to validate their own workflow. However, it is our responsibility to ensure that workflows generated by Cumulus AI are consistent with the input data. The workflow generated should match the procedure the user uploaded.

How will Cumulus AI continue to improve its security posture in the future?

As we further develop Cumulus AI, our intention is to build a library of procedures. This "procedure center" will use an LLM that is fully trained in industry procedures to generate workflows. We will accomplish this by using a RAG (retrieval augmented generation) model, where augmented data and user feedback helps continuously improve our workflows. This will ensure that workflows generated by Cumulus AI continue to improve for all your work activities. Your data will only be included in the RAG on an opt-in basis.

Download on the App Store

GET IT ON Google Play