Should Employers Allow Open AI Models at Work?

By Jordan Lanning

4/20/2025

Introduction:

Artificial Intelligence has been around since the 1950s, but in recent years, we have seen significant increases in its capabilities due to technological advancements. So much so that we have free open source models available for the public. The models have advanced to where you can see high levels of accuracy for a variety of industries or topics. Today, AI models can teach university course material, produce 100-page reports, and much more. Some AI applications can fabricate realistic video content that are so good it can deceive the untrained eye.

But this article will mainly focus on open AI and typical organizational work.

My Position:

I wholeheartedly believe that companies should not outright restrict the use of AI models like ChatGPT or Copilot. A year ago, I might have disagreed with my thoughts today, but I have heavily used AI to teach and walk me through complex concepts or projects – like passing the CompTIA CySA+ exam and deploying servers in Azure. With that said, there should be some consideration. There are both positive and negative effects of AI in the workplace. Depending on what the organization does can impact restrictions or limitations. As an employer or manager, you should also understand the end user's intent behind the tool utilization.

Use Cases and Considerations:

Why is my employee using it? If your employee is using it as a teaching mechanism so that managers aren't flooded with too many questions throughout the day, then this seems appropriate. For instance, an engineer can't find the specific script to run a program so the employee then asks open AI for that clarification.

What information is the employee feeding it? Employees should increase data loss prevention (DLP) awareness and not feed any personally identifiable information, cardholder data, or proprietary information directly into a AI model. Employers can ensure that anonymized data can be used to replace real or live data.

Are you relying on AI to do all your work? This probably wouldn't be the most ideal situation in most circumstances. As mentioned earlier, AI models are not completely accurate - due to outdated data or lack of context of a query. Therefore, employees will not be able to identify errors in AI if they don't have the working knowledge to not forward inaccurate data produced by AI models.

Does your company manage secret or top secret information? You are more than likely still use it with careful consideration. We don't truly know how our data we feed the model is handled,

which would be extremely problematic. Companies that fall into this category have the option of creating their own working AI model and privately manage the data to better suit their needs.

Are employees using it to save time? This is where I find the most use, but you can save so much time researching or developing tasks. An open AI model can write a length research paper by pulling from substantial amounts of open source information, while I wouldn't recommend using it for your entire report. However, I would use it to consolidate resources and articles to begin my research. An employee theoretically could spend 30 minutes searching within the wrong search parameters – this certainly is not a good use of time.

Security & Policy Considerations:

While this might not be all an employer should consider, it is a starting point to understand how you can integrate open AI models into your daily work. Confirm with your security and legal teams to ensure that you set appropriate policies that address your companies needs. At minimum, maintain an internal AI usage log for reference.