



Code of Conduct



MÉRIEUX NUTRISCIENCES

PUBLIC DOMAIN GENERATIVE AI

TOOLS USAGE POLICY

PUBLIC DOMAIN GENERATIVE AI TOOLS USAGE

(January 2025 – V.2)

1. OBJECTIVE

The purpose of this policy is to establish guidelines for the use of publicly available Generative AI tools, such as Chat GPT, within Mérieux NutriSciences. This policy aims to mitigate the legal and business risks associated with using Generative AI, particularly regarding the use of confidential and sensitive business, customer, and personal information, as well as intellectual property risks. By adhering to this policy, employees and authorized users can make informed and responsible decisions when utilizing AI tools. This policy is intended to be read in conjunction with the Company's Code of Conduct and other compliance policies.

2. LEGAL AND BUSINESS RISKS

The following legal and business risks must always be kept in mind when using Generative AI tools.

2.1. Confidential and Sensitive Information - Personal data

2.1.1. Using Generative AI tools can risk exposure of confidential and sensitive business, customer, and personal information. All data and information shared with Generative AI tools through prompts, search queries, and conversations become part of the public domain.

2.1.2. Generative AI tools may automatically collect and reuse without your consent information about your use, including information you explicitly share, such as anything you type into a conversation, as well information you implicitly share, such as your location.

2.2. **Intellectual Property.** Generative AI tools can generate content that may be subject to intellectual property protection. Work products that contain outputs from Generative AI may not be protected by copyright laws. Similarly, content derived from Generative AI may be derivative of copyrighted materials used to train the AI system. Unauthorized use or

dissemination of copyrighted content can lead to legal liabilities and damage the Mérieux NutriSciences' reputation.

2.3. **Reliability.** Generative AI tools may be limited in knowledge of the world and events and may produce incorrect or biased responses that could be harmful. Some of them are based on information that is out of date or incomplete.

2.4. **Cybersecurity.** As Generative AI tools are able to code, they are also able to detect errors and vulnerabilities in the code and such code analysis could potentially be used to guide hackers in their search for vulnerabilities.

3. USAGE GROUPINGS FOR GENERATIVE AI

3.1. **Prohibited Uses.** The following use cases are strictly prohibited and should not be performed using Generative AI tools:

3.1.1. *Illegal and Unethical Activities.* The use of any output created by Generative AI tools that causes or promotes illegal or unethical activities, including but not limited to hacking, fraud, harassment, defamation, intellectual property infringement, personal data breach and any other activities in violation of local, national, or international laws, is strictly prohibited.

3.1.2. *Discrimination and Hate Speech.* The use of any output created by Generative AI tools should not promote discriminatory, offensive, or hate speech. Any use that may infringe upon the rights, dignity, or well-being of individuals or groups based on their race, ethnicity, gender, religion, disability, or any other protected characteristic is strictly prohibited.

3.1.3. *Reliance on Confidential or Sensitive Information.* Sharing of confidential, proprietary, or personal information when interacting with Generative AI is strictly prohibited. Information that may never be disclosed includes but is not limited to: proprietary information and data, trade secrets, and know-how belonging to either Mérieux NutriSciences or its customers or suppliers. Similarly, employees may not request or disclose any personal data (including that of customers, vendors, and co-workers) protected by data protection and privacy laws.

3.1.4. *Legal advice:* Employees should not rely on Generative AI's responses as a source of legal advice. Generative AI is a language model and cannot provide specific legal advice for a given situation. It is best to consult legal counsel for any legal questions or concerns.

Ultimately, each employee, and the Company, is responsible for the use of any output created by Generative AI. Employees must be cautious while using Generative AI tools not to elicit illegal or unethical activities.

3.2. **Permitted Uses with Authorization.** Keeping in mind the legal, ethical, and business risks already identified, the following use cases may be permitted upon authorization:

3.2.1. *Coding*. Prior approval by the IT manager should be obtained before sharing coding with AI tools. Sharing software code should be carefully done and in any case limited to small portions of code or specific functions. Coding only small portions can help mitigate the potential exposure of the entire codebase, reducing the risk of intellectual property violations and maintaining data security. In any case, code suggested by AI tools must be reviewed by an IT team manager prior to deployment.

3.2.2. *Decision Making*. Generative AI tools should not be solely relied upon for advice, decisions, and diagnostics. Rather, Generative AI can assist in research and analysis. Final decisions should be made by qualified individuals and professionals should be consulted.

3.3. **Generally Permitted Uses without Authorization**. The following use cases are permitted, keeping in mind the legal, ethical, and business risks already identified:

3.3.1. *Research and Analysis*. Generative AI tools can be used to support research and analysis, enabling faster data processing, pattern recognition, and generating insights. They can assist in identifying trends, making predictions, and informing decision-making processes. Generative AI results may not be error free and should be independently reviewed by qualified professionals prior to use or reliance.

3.3.2. *Customer Support and Service*. Generative AI tools can enhance customer support and service by providing quick and accurate responses to common inquiries, improving response times, and offering personalized assistance as long as the request is made in an anonymized way and the issues faced with our customers are kept confidential. Human supervision and intervention should be in place to handle complex or sensitive customer issues.

3.3.3. *Content Generation and Enhancement*. Generative AI tools can be utilized to generate content such as articles, blog posts, or creative works. They can also enhance existing content by suggesting improvements or generating alternative ideas.

In all cases, human oversight and review of AI outputs is necessary to ensure the quality, accuracy, and adherence with internal guidelines.

4. COMPLIANCE AND TRAINING.

Employees and authorized users must comply with this policy and receive appropriate training on the responsible and ethical use of Generative AI tools. The policy will be periodically reviewed, and any updates or revisions will be communicated to all relevant personnel. By following this Generative AI Usage Policy, we can create mindful practices that harness the benefits of Generative AI tools while minimizing the legal and business risks to our company.



5. RAISING QUESTIONS AND REPORTING IDENTIFIED RISKS.

This Policy does not address every situation you may encounter at work. If there is a situation that you think may pose a risk and you are unsure about how to handle it, you should seek guidance. Support is available to you from your manager and from the Legal Affairs and Compliance Department.

Your questions or concerns will remain confidential to fullest possible extent and will receive quick and appropriate follow-up.

* *
*