

Security Policy Usage of **Artificial Intelligence based Large Language Models**

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| **Richtlinie Usage of Artificial Intelligence based Large Language Models** | |  |
| Nummer | [Nummer] | |
| Erlassen am | 04.07.2022 | |
| Durch | Chief Information Security Officer | |
| Inkrafttreten | 01.01.2024 | |
| Geltungsbereich | SÜDVERS Holding GmbH & Co. KG und deren Tochtergesellschaften mit Mehrheitsbeteiligung, sowie die SÜDVERS International GmbH | |
| Thema | Compliance | |
| Verantwortliche Funktion | Informationssicherheit | |
| Verantwortliche Person | Dirk Franken | |
| Übergeordnete Vorschrift | Informationssicherheitspolitik | |
| Ersetzt | n/a | |
| Mitgeltende Dokumente |  | |
| Gültigkeit | Bis auf Widerruf | |
| Letzte Überprüfung | 14.07.2025 | |
| Nächste Überprüfung | 07.01.2026 | |
| Publikation | SÜDVERS Intranet | |
| Klassifizierung | Intern | |
| Archiv | Dokumentenverwaltungssystem | |
| Ordnungssystem | [Ordnungssystem] | |
| Sprachen | Englisch | |
| Formate | Online | |
| Bemerkungen |  | |

Table of Content

[1 Purpose: 4](#_Toc146621884)

[2 Objective: 4](#_Toc146621885)

[3 AILLM Acceptable Use Policy 5](#_Toc146621886)

[3.1 Authorized AILLM tools 5](#_Toc146621887)

[3.2 Authorized use 5](#_Toc146621888)

[3.3 Responsible use: 5](#_Toc146621889)

[3.4 Personal Use 6](#_Toc146621890)

[3.5 Unauthorized use 6](#_Toc146621891)

# **Purpose**:

The purpose of this information security policy is to establish guidelines for the use an artificial intelligence based large language model (AILLM), such as of ChatGPT, Meta LLaMA, Google Bard, Microsoft Bing Chat, or other similar tools, by all those working within SÜDVERS. This policy is designed to ensure that the use of AI is ethical, lawful, and in compliance with all applicable laws, regulations, statutory requirements and SÜDVERS internal policies.

Ein Bild, das Text, computer, Computer, Screenshot enthält.

Automatisch generierte Beschreibung

“I cannot process, store, or share confidential information. My primary function is to provide information and answer questions to the best of my knowledge and abilities. If you have any concerns about confidentiality or data security, please avoid sharing sensitive or private information with me or any other online AI model. It's essential to follow best practices for information security and data privacy when using AI systems.” (ChatGPT, 23.09.2023)

# **Objective**:

This AILLM policy defines the rules and guidelines for the use of AILLM tools by all those working within SÜDVERS. The purpose of this policy is to ensure the security of our SÜDVERS’ and its customers’ information and data, as well as to maintain a professional and respectful environment for our users.

# AILLM Acceptable Use Policy

## Authorized AILLM tools

To ensure compliance with other information security policies and to ensure confidentially of information and compliance with regulatory requirements (such as GDPR) it must be ensured that for business purposes only AILLM tools are being used that are formally approved by both our IT department and information security function. In addition, it is essential that these tools are only run on secured browsers (such as MS Edge on our Surfaces or Citrix computers).

## Authorized use

Employees are authorized to use formally authorized AILLM tools for work-related purposes. This includes tasks such as research, data analysis, and communication with clients and colleagues.

AILLM tools can support new employees during the onboarding process by answering their questions, providing training materials, and offering guidance. It can offer personalized learning recommendations and assist in knowledge transfer.

AILLM tools can be used to generate content for various purposes, such as writing blog posts, drafting emails, creating social media updates, or developing marketing materials. It can help with brainstorming ideas, proofreading, and improving the overall quality of written content.

In addition, not limited to, AILLM tools can be used to

* serve as a virtual assistant to handle customer queries, providing real-time responses and assistance. It can handle frequently asked questions, provide troubleshooting tips, and offer personalized recommendations.
* automate routine and time-consuming tasks, allowing employees to focus on more value-added activities. This boosts productivity, efficiency, and employee satisfaction.
* analyze vast amounts of data, providing valuable insights for decision-making, identifying patterns, predicting trends, and driving innovation.
* optimize workflows by streamlining processes, identifying bottlenecks, and suggesting improvements, thereby improving overall operational efficiency.
* assist in real-time language translation. It can help overcome language barriers and enable effective communication across different languages.

## Responsible use:

* **Proofing:**All AI-generated content must be proofread and reviewed and edited for accuracy by a human before being published or shared. This includes checking for spelling errors, grammar mistakes, and factual inaccuracies. Employees must adhere to copyright laws when utilizing AILLM. It is prohibited to use AILLM to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material. If an employee is unsure whether a particular use of AILLM constitutes copyright infringement, they should contact the legal department for guidance. All AI-generated content should be clearly labeled as such, and the use of solely AI generated content should be transparent to employees and customers.
* **Editing:**AI-generated content must be edited to ensure that it is well-written, coherent, and engaging. This includes ensuring that the content is structured in a logical manner and that it is appropriate for the intended audience.
* **Fact-checking:**AI-generated content must be fact-checked to ensure that all information is accurate and up to date. This includes verifying sources, checking statistics, and ensuring that any claims made in the content are supported by evidence.
* **Starting point, not the finished product:**AI-generated content should be viewed as a starting point, not the finished product. While AI can provide a valuable tool for generating content, it cannot replace the creativity and critical thinking skills of human writers and editors.

## Personal Use

Employees may use AILLM tools of their own choice for personal purposes but must not use these for any business-related activities or activities that may violate SÜDVERS policies, such as harassment or discrimination.

## Unauthorized use

* Employees must not use any not formally approved AILLM tools for business purposes.
* Employees must not use AILLM tools for any activities that may be unrespectful, illegal or unethical, including but not limited to spreading false information, engaging in cyberbullying or harassment, or attempting to gain unauthorized access to any systems or networks.
* AILLM tools must not be used to intrude on employee privacy rights, such as unauthorized monitoring of communications, personal devices, or sensitive personal information.
* AILLM tools must not be used for unethical data collection practices. This includes obtaining personal information without consent, collecting excessive or irrelevant data, or leveraging AI to exploit user privacy for unauthorized purposes. Such practices not only violate privacy regulations but can also lead to distrust among employees and customers, resulting in reputational damage and potential legal repercussions.
* Employees must not disclose any information above the classification label “restricted” while using AILLM tools. In addition, employees should also ensure that they are not discussing any matters above the classification category “internal” in areas where others may overhear or oversee their conversations.
* Employees must not use AILLM tools to generate internal communications, policies or documentation, or any other materials that are intended to be used in connection with the running of businesses.
* Employees must not use AILLM tools to conduct business. This includes using such tools to generate any kind of customer communication, even as a starting point.