# ARTIFICIAL INTELLIGENCE USAGE POLICY - TEMPLATE

## I. PURPOSE

The purpose of this policy is to define guidelines for the appropriate use of Artificial Intelligence (AI) tools at $COMPANY. It aims to encourage the efficient and secure utilization of AI, including generative AI programs and ChatGPT, while mitigating associated risks.

## II. SCOPE

This policy applies to all employees of $COMPANY and covers the use of all AI tools provided by the company, including but not limited to generative AI programs and ChatGPT.

## III. POLICY

### 1. Authorized Use

Only employees authorized by $COMPANY and who have received the necessary training are permitted to use AI tools. This authorization process is necessary to ensure that users understand the capabilities and limitations of these tools and use them effectively and responsibly.

Unauthorized use includes, but is not limited to, usage by non-authorized personnel, utilization beyond one's scope of work, or employing the tools in manners inconsistent with this policy or other company guidelines. Any suspected unauthorized use should be reported to the relevant supervisory personnel or IT security team promptly. Unauthorized usage may lead to disciplinary action, up to and including termination of employment.

### 2. Data Security and Confidentiality

Preservation of company data security, intellectual property, and confidentiality is paramount in all activities, including the use of AI tools. As these tools learn and generate content based on the input data, it is crucial that users avoid inputting or sharing sensitive information, such as customer data, confidential contracts, details about partnerships, projects, work statements, or any other proprietary information.

Furthermore, users must respect the legal and ethical boundaries concerning data privacy. If an employee is unsure whether specific information is appropriate to use with the AI tool, they should consult their supervisor or the legal department. Violations of data security and confidentiality guidelines may result in disciplinary action, up to and including termination of employment.

### 3. Use of AI Tools as Supplemental Resources

AI tools are not stand-alone solutions but are part of a wider set of resources to assist employees in their roles. They should be used to supplement, not replace, traditional methods of problem-solving and decision-making.

The output of AI tools should always be supplemented with business logic. For instance, if an AI tool generates a suggestion or plan, users should critically evaluate the suggestion using their understanding of the company's business model, strategy, and market conditions.

Furthermore, collaboration with colleagues is encouraged to gain different perspectives, double-check the AI tool's outputs, and reduce the risk of errors.

Additionally, employees should appropriately validate the output of AI tools. This could involve cross-verifying the information with other reliable sources, performing rigorous testing if feasible, or consulting experts when necessary.

Using AI tools as a supplement ensures that we retain human judgement and oversight in our processes, thereby maximizing the value of these tools while minimizing the associated risks.

**4. Risk Assessments for Artificial Intelligence Usage**

In the course of using AI tools, employees should always be aware of the inherent risks these technologies pose. These may include potential inaccuracies or misinterpretations in AI-generated content due to lack of context, legal ambiguities concerning content ownership, and possible breaches of data privacy. As such, a critical attitude towards AI outputs is required at all times.

To ensure that risks associated with AI usage are effectively managed, it is the responsibility of management to incorporate AI-specific risk assessments into the company's broader risk management procedures. This includes continually evaluating and updating protocols to identify, assess, and mitigate potential risks, with considerations for changes in AI technology, its application, and the external risk environment. This also necessitates periodic training and awareness sessions for employees to ensure they stay informed about these risks and the steps needed to mitigate them.

**5. Use of Third-Party AI Platforms**

Employees should exercise caution when using third-party AI platforms due to the potential for security vulnerabilities and data breaches. Before using any third-party AI tool, employees are required to verify the security of the platform. This can be done by checking for appropriate security certifications, reviewing the vendor's data handling and privacy policies, and consulting with the company's IT or cybersecurity team if necessary.

Moreover, data shared with third-party platforms must comply with the guidelines outlined in Section B (Data Security and Confidentiality). In situations where employees are unsure about the use of a third-party platform, they should seek guidance from their supervisors or the IT security team.

**6. Use in Communications**

AI tools, when used appropriately, can aid in facilitating efficient internal communication within $COMPANY. This includes drafting emails, automating responses, or creating internal announcements. However, while using AI for these purposes, it is crucial that employees adhere strictly to the company's policies on harassment, discrimination, and professional conduct.

AI-generated communication should be respectful, professional, and considerate, mirroring the high standards of interpersonal communication expected at $COMPANY. Any misuse of AI tools for communication, including any language or behavior that violates company policies, will be treated as a serious violation and may lead to disciplinary action, up to and including termination of employment.

**7. Use in Research and Development**

AI tools, including but not limited to language models and machine learning algorithms, can serve as valuable assets in streamlining the research and development processes within $COMPANY's portfolio of businesses. They can expedite data analysis, facilitate trend identification, accelerate prototyping, and augment creative brainstorming.

However, when employing AI tools for R&D purposes, all usage must strictly align with our intellectual property and data security policies. Intellectual property generated through the use of AI tools remains the property of $COMPANY, and any misuse or unauthorized distribution of this property could lead to severe disciplinary actions.

Additionally, any data used in conjunction with AI tools for R&D, whether it's proprietary, customer-related, or otherwise sensitive data, must be handled according to our data security policies. This includes ensuring appropriate anonymization or pseudonymization of sensitive data, and proper access controls to ensure only authorized personnel have access to such information.

**8. Non-Personal Use**

The AI tools provided by $COMPANY are for business use only and should not be used for personal activities. This policy is in place to ensure the maintenance of a professional environment, the preservation of company resources, and to prevent potential legal and security risks.

Personal use of these tools could potentially involve sharing of inappropriate or sensitive content, misuse of company time and resources, and potential breach of data privacy regulations. Therefore, employees are expected to refrain from using AI tools for non-work-related tasks or discussions.

In instances where the line between professional and personal use might be blurred (e.g., professional development), employees are encouraged to seek approval from their supervisor or the appropriate department. Any misuse of AI tools for personal purposes can result in disciplinary action, up to and including termination of employment.

**9. Monitoring**

$COMPANY reserves the right to monitor all interactions with AI tools for the purpose of ensuring compliance with this policy.

**10. Violations**

Breaches of this policy may lead to disciplinary action, including potential termination of employment.

## IV. POLICY COMPLIANCE

Compliance with this policy will be monitored regularly by $COMPANY. Any policy breaches identified will be addressed and remedied promptly.

## V. REVIEW AND REVISION

This policy will be reviewed and updated periodically to accommodate changes in technology, business needs, or legal requirements.