**AI Policy Template**

**[Company Name]**

This policy outlines how AI tools should be used across the company. It helps employees understand what’s allowed, what’s not, and how to use AI responsibly and securely in their work.

## 1. Purpose and scope of the policy

This policy outlines how artificial intelligence (AI) tools may be used within [Company Name]. It applies to all employees, contractors, and third-party vendors who use AI tools in the course of their work with or for the company. The goal is to support responsible, secure, and ethical use of AI while minimizing risks.

## 2. Definitions of AI tools and technologies

For clarity, here are some definitions we’ll use throughout this policy:

* **Artificial intelligence (AI):** Software that mimics human intelligence to perform tasks like analyzing data, making decisions, or generating content.
* **Generative AI:** A type of AI that can produce new content, such as text, images, or code (e.g., ChatGPT, Midjourney, GitHub Copilot).
* **Machine learning:** Algorithms that improve through experience and data exposure, often used behind the scenes in AI tools.

These tools include, but aren’t limited to, public or enterprise versions of language models, image generators, automation platforms, and internal AI applications.

## 3. Authorized use guidelines

Employees are encouraged to explore AI tools for efficiency and creativity—but with limits:

✅ Acceptable uses:

* Summarizing meeting notes or internal reports
* Drafting first versions of internal communications
* Automating repetitive tasks (e.g., formatting, tagging).

🚫 Unacceptable uses:

* Generating client-facing content without human review or approval
* Using AI to replace human judgment in decision-making processes
* Uploading or training tools on sensitive or proprietary data.

If in doubt, check with your team lead or IT contact before using any AI tool for a new purpose.

## 4. Data privacy and security considerations

Publicly available AI tools should never be used to process sensitive information. Such information includes but is not limited to:

* Customer data
* Financial records
* Personal employee information
* Legal documents.

All AI tools must be used in line with our existing data protection policies. Enterprise tools must be vetted by IT for security compliance before adoption.

## 5. Ethical use guidelines

AI use in the organization should reflect our values. This means:

* Avoiding any content that could be biased, discriminatory, or offensive
* Not using AI-generated content to mislead others
* Respecting copyrights and intellectual property — there must be no copying or adapting third party content without permission.

When in doubt, assume a human touch is still needed.

## 6. Human oversight requirements

AI tools can be used to assist you, but they shouldn’t replace human accountability. This is especially important in the following areas:

* Recruitment and hiring
* Employee evaluation
* Customer interactions
* Strategic decisions.

A human staff member must always review and approve any AI-generated output used in these areas.

## 7. Risk management instructions

If you notice anything amiss — such as an incorrect output, signs of bias, or a security concern — report it promptly. Contact [Risk Contact Name or Team] at [Email/Slack/etc.], and document the issue as part of our regular risk tracking process.

## 8. Use limitations and prohibited use guidelines

The following actions are strictly forbidden:

* Creating deepfakes, impersonating individuals, or fabricating information
* Using AI tools for personal gain during work hours or on company systems
* Circumventing laws or compliance requirements using AI
* Developing or deploying unapproved AI applications within the company infrastructure.

Violations will result in disciplinary action, which may include termination of employment in more serious cases or after repeat offences.

## 9. Training and awareness directions

We will provide training to help you get the most out of AI safely and ethically. New employees must complete a basic AI training module during onboarding, and additional resources will be shared through / on [platform: LMS, intranet, etc.].

If you have any questions or concerns, contact [IT/Security/HR] or visit [internal resource hub].

## 10. Policy review and update process

This policy will be reviewed and updated every [6 or 12] months, or sooner if AI capabilities or risks shift significantly. Employees are encouraged to share feedback so the policy stays up-to-date, accurate, and useful.



