Policy on the Use of Artificial Intelligence Tools

[Company name] | Version 1.0 | Effective from: [date] | Document owner: [full name, job title]

This template is for guidance only and does not constitute legal advice. Complete or delete the items in square brackets. Before introducing the document, consult a lawyer, especially if you process personal data or operate in a regulated sector.

1. Purpose and scope

This policy sets out how employees and associates of [Company name] may use artificial intelligence (AI) tools at work, so that the company can benefit from their usefulness without exposing itself to data leaks, wrong decisions and breaches of regulations.

It applies to everyone working for the company (employment contracts, civil-law contracts, interns) and to all AI tools, including text and image generators, assistants built into office suites, translators, transcription tools and agents that automate tasks. It also covers free tools and private accounts used for work tasks.

2. Definitions

AI tool	Any software or service that generates content, answers, classifications or decisions using machine learning models.
Approved tool	A tool entered on the List of Approved AI Tools and used only on a company account.
Shadow AI	The use of AI tools for work tasks without the organisation's knowledge and approval, including on private accounts.
AI topic owner	[Full name, job title]. The person responsible for implementing and enforcing the policy.

3. AI topic owner

The AI topic owner keeps the register of AI tools, approves and withdraws tools, answers employees' questions ("may I use this for…"), receives incident reports and presents a short report to the board once every [6] months. This person has the right to suspend the use of a tool until the risk has been clarified.

4. Approved tools

- For work tasks, only tools from the List of Approved AI Tools, maintained by the AI topic owner, may be used.
- Tools are used only on company accounts. Private accounts and free versions must not be used to process company data.
- Want to use a new tool? Report it to the AI topic owner. You will receive an answer within [5] working days. Until a decision is made, you do not use the tool with yellow or red data.
- Approval is preceded by a vendor assessment using the AI Tool Vendor Assessment Checklist and an entry in the register.

5. Data classes

Before pasting anything into an AI tool, decide which class the data belongs to.

Class	Examples	Rule
GREEN	Public content: website, published materials, the public version of the offer, general knowledge questions.	Any approved tool.
YELLOW	Internal documents without personal data: procedures, meeting notes without client data, draft offers without names or individual prices.	Approved tools only, company account; you check the results before use.
RED	Personal data of clients and employees, financial data, trade secrets, source code, client contracts, passwords and access keys, confidential information covered by a contract.	Prohibited, unless the AI topic owner has approved the specific use in writing after a risk assessment.

In case of doubt, apply the higher data class.

6. Rules of use

Do

- check the tool's output before using it: facts, figures, names, quotations, links;
- anonymise data if the task requires it and anonymisation does not change the meaning of the task;
- report to the AI topic owner any new uses that affect clients or employees.

Do not

- enter red data into AI tools without approval;
- use AI to make or prepare decisions about people (recruitment, employee evaluation, dismissals, client scoring) without the consent of the board and legal consultation;
- send clients AI-generated replies without human verification;
- connect AI tools to mailboxes, drives, financial systems or CRM without approval of the scope of permissions;
- bypass the tools' safeguards or use prohibited tools.

7. Responsibility for the result

A person who sends, publishes or uses content prepared with the help of AI is responsible for its content as if they had written it themselves. Saying that "the tool said so" does not change this responsibility.

8. Content published externally

Images, recordings and texts generated by AI that we publish externally are labelled where the regulations require it (in particular Article 50 of the AI Act) or where the lack of a label could mislead the audience. Report any doubts to the AI topic owner before publication.

9. Incident reporting

We regard the following in particular as an incident: pasting red data into an unapproved tool, sending a client incorrect AI-generated content, unauthorised access to a tool account, and the loss of a device with a logged-in account. Report an incident without delay, no later than [24] hours after noticing it, to

[email / telephone]. A report made in good faith is not grounds for consequences for the person reporting. The AI topic owner assesses whether the incident must be reported to the data protection officer, to the Polish data protection authority (Urząd Ochrony Danych Osobowych, UODO) or to the client.

10. Training

Everyone who uses AI tools completes initial training ([60] minutes) covering this policy, the data classes and examples from our work. We repeat the training once every [12] months and whenever the policy changes materially. The list of participants is kept by [the AI topic owner].

11. Review and sanctions

We review the policy every [6] months, and whenever the regulations change or a new type of tool is introduced. A breach of the policy may result in withdrawal of access to the tools and in the consequences provided for in the work regulations (regulamin pracy) or in the contract.

Approved by (board): [full name, date, signature]	AI topic owner: [full name, date, signature]