

Document ID: E3	Document name: AI Policy
Version: 1.0	Owner: CEO
Date: 14-11-2025	Classification: Internal

LOGO

COMPANY NAME

AI Policy

[COMPANY]

Version: 1.0

Approved by management: NOT YET APPROVED

Document ID: E3	Document name: AI Policy
Version: 1.0	Owner: CEO
Date: 14-11-2025	Classification: Internal

LOGO

This template was created by the people of ICT Institute. You can find the latest version and other templates here: <https://ictinstitute.nl/free-templates/>

*You can use this template freely under the Create Commons Attribution license
<https://creativecommons.org/licenses/by/4.0/>*

You can do the following with the templates:

Share. You can share the templates and any documents made with these templates freely, with any one that you want to share it with.

Adapt. You can make new documents based on the templates, make changes, add elements or delete elements as much as you want. You can even do this in commercial organisations or for commercial purposes.

If you are a customer, you do not have to mention ICT Institute anywhere. If you are not a customer, you must keep the text "create by the people of ICT Institute" somewhere

Note that the use of these templates is of course at your own risk. Note also that the ISO standards are copyrighted. You must buy the standard from NEN or ISO before using it.

1 Purpose and Context

The rapid growth of powerful, user-friendly AI tools has led to widespread use across many tasks. People rely on chatbots (e.g., ChatGPT, Gemini) for questions and summaries, use generative tools (e.g., DALL·E, Midjourney, Veo) for creating content, and coding assistants (e.g., Copilot, Claude) to develop or debug software. While these tools offer significant benefits, they also introduce specific risks. Users must understand these risks and apply AI responsibly. This policy outlines the principles and rules for acceptable use of AI systems.

2 Scope

This policy applies to all Company employees and to external contractors working with Company staff.

It covers the use of any public or third-party AI system, such as those listed above, by all departments and on all Company information assets. It does not apply to formally approved or internally developed AI systems that have their own usage guidelines.

3 Acceptable use principles

- **AI tools are not a substitute for human judgment or creativity.** Most AI systems generate outputs using statistical patterns from previously ingested data. They cannot fully replace human reasoning, judgment, or creativity. For example, employment or promotion decisions must never be made solely by AI.
- **Always verify the correctness of AI output.** Generative systems may produce “hallucinations” - plausible but incorrect or fabricated information. They may also rely

Document ID: E3	Document name: AI Policy
Version: 1.0	Owner: CEO
Date: 14-11-2025	Classification: Internal

LOGO

on outdated, biased, or inaccurate training data. Always verify AI-generated content for correctness, appropriateness, and potential copyright issues.

- **Ensure the output does not copy or infringe existing work.** Check that AI-generated content does not closely resemble the work of living artists, copyrighted images, or text from a single identifiable source. Use search engines or reverse-image tools when necessary. Do not ask AI systems to copy, imitate, or modify protected works.
- **Do not share confidential information with AI tools.** Many AI providers store and reuse input data for model improvement. Do not enter personal data, confidential business information, passwords, configuration files, or any other sensitive details. Assume that anything provided to a public AI service could become publicly accessible.
- **Be transparent about AI use.** Clearly disclose when AI has contributed to your work. Do not pass off AI-generated content as solely your own. Certain uses, such as public-facing customer support chatbots, may require disclosure under regulations like the EU AI Act. If you use AI to generate content (e.g., as placeholder text or imagery), note that AI was used.

4 Privacy aspects and AI Act

Personal data must not be shared with external AI tools or services. You must remove all personal data from any document before providing it as input to an AI system. Data protection laws, such as the GDPR, apply fully to any data used with AI systems. Therefore, employees must ensure that personal data is used only for the purposes for which it was originally collected.

If, as a developer, you introduce a new AI-powered feature in our platform, this may constitute a new use of personal data. In such cases, a Data Protection Impact Assessment (DPIA) may be required. Contact the Information Security team when planning new or innovative uses of personal data so they can determine whether a DPIA is necessary. The team will also evaluate whether the new use is high-risk or restricted under the EU AI Act, and whether additional impact assessments are needed.

If the AI Act applies, the Information Security team will consider, among other things:

- Human oversight of any significant decisions made by AI
- Risks of bias, discrimination, or unfair outcomes
- Logging, monitoring, and auditability requirements
- Transparency obligations, e.g., informing users when they are interacting with a chatbot rather than a human

Document ID: E3	Document name: AI Policy
Version: 1.0	Owner: CEO
Date: 14-11-2025	Classification: Internal

LOGO

5 AI and coding

AI tools may be used to support software development tasks, just like other external resources (e.g., search engines or technical websites). However, developers must carefully review all AI-generated code to ensure that it does not introduce security risks such as backdoors or unexpected calls to external services. Developers must also test the code to confirm that it functions as intended. AI-generated code can contain bugs or vulnerabilities, just like any other code.

6 Approved AI services

The Company will carefully assess all suppliers, including AI service providers, before their services are used. If you require an AI service, contact the Information Security team and specify which service you need and which supplier you are considering. The team will use the existing supplier review process to determine whether the supplier is suitable and reliable. The review will consider:

- Supplier reliability, including relevant certifications. ISO 27001 is preferred for EU-based suppliers, while SOC 2 is acceptable for US-based suppliers.
- GDPR compliance if personal data will be shared. This requires either an EU-based supplier or a US-based supplier with a strong privacy policy and a Data Processing Addendum (DPA) that mentions Standard Contractual Clauses (SCCs).
- Cloud-related risks if the AI provider is a cloud service, including safe use, maintenance, availability, and exit strategies.

If the planned use of AI represents a major change, we will create a project plan and assign a project manager.

Employees must not independently introduce AI services into Company operations. Without explicit approval, AI tools may only be used for personal learning or experimentation, and only with non-sensitive data.

7 Training and awareness

The Company will regularly conduct surveys to understand which AI tools employees use and for what purposes. These tools and their use cases will be evaluated for security and privacy risks. Approved tools and permitted use cases will be added to a Company whitelist, and licenses will be obtained where necessary.

The Security Officer will include AI awareness in the Company's information security awareness training and ensure that this policy is accessible to all staff. Additional, role-specific training will be provided to employees who use, oversee, or implement AI systems when relevant.

Document ID: E3	Document name: AI Policy
Version: 1.0	Owner: CEO
Date: 14-11-2025	Classification: Internal

LOGO

8 Appendix

References

This policy is inspired by:

<https://futurium.ec.europa.eu/en/european-ai-alliance/document/writingorganizational-ai-policy-first-step-towards-effective-ai-governance>

<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

GDDPR Article 5. Principles relating to processing of personal data: purpose limitations, integrity and confidentiality. Relevant for not sharing confidential information with AI tools.

GDPR Article 6. Lawfulness of processing: you need a legal basis before feeding personal data into any AI or analytics system. This is relevant for with the introduction of AI powered features by developers.

GDPR Articles 12-14. Information to data subjects: be transparent about use of AI with users.

GDPR Article 28. Use of processors: AI services need to be approved by IT and Legal departments due to potential need for DPAs or transfer of data requirements.

AI Act Articles 52-53. Transparency obligations: Users must be informed when interacting with AI chatbots.

AI Act Article 6 (annex III). When an AI system can be high-risk: needs review by IT/relevant department

This policy implements parts of requirements of following controls in annexes A5 and A8:

5.10 Acceptable use of information and other associated assets, 5.14 Information transfer, 5.23 Information security for use of cloud services, 5.34 Privacy and protection of personal identifiable information (PII), 8.28 Secure coding, 8.25 Secure development life cycle, 8.26 Application security requirements

Guidelines for assessing the use of AI

Product owners should consider the following when deciding whether to use AI and evaluate these aspects in any AI related project plan.

- **Transparency/Explainability/Auditability:** defines both transparency of an organization, and transparency of an algorithm, and aims at making information in and about AI systems understandable to non-experts and useful for audits.
- **Safety/Security:** requires AI systems to be protected against external attacks, including safety mechanisms throughout their lifecycle, and ensuring they function appropriately even under adverse conditions. This includes regular risk assessments and adherence to data security regulations.
- **Robustness/Reliability:** requires AI systems to operate reliably, performing consistently according to their intended purposes while minimizing risks, and display technological robustness to misuse or external attacks.

Document ID: E3	Document name: AI Policy
Version: 1.0	Owner: CEO
Date: 14-11-2025	Classification: Internal

LOGO

- **Justice/Equity/Fairness/Non-discrimination:** defines AI systems to be non-discriminatory and ensure bias mitigation, means that individuals should be objection to the same, fair algorithmic treatment regardless of their characteristics.
- **Privacy:** prioritizes the individual's right to choose if and to what extent they want to expose themselves to the world, and relates to data protection concepts, such as anonymity and informed consent.
- **Accountability/Liability:** aims at defining roles and responsibilities for the adherence of compliance with both own policies, and law, and holding them accountable for the impacts caused by the development or use of technologies.