AI POLICY

EDITION 2025

EWES GROUP

CONTENTS

PURPOSE AND SCOPE

PURPOSE

The purpose of EWES' AI Policy is to ensure that our employees have sufficient AI competence to understand systems, contexts, and the impact on individuals and groups.

Supported by the EU AI Act, our policy promotes transparency, responsible use, and regulatory compliance in the use of generative AI within the company.

SCOPE

This policy applies to:

- AI-supported text processing, language models, and image generation for marketing purposes
- AI-assisted machine programming and control of production-specific machinery
- AI functionalities on the company website, such as calculation and modelling
- The use of AI as a decision-support tool

APPLICABILITY

BUSINESS AREAS

This policy applies to all employees of EWES AB who come into contact with AI in the course of their professional duties.

APPLICATION IN THE ORGANISATION

- All employees are informed about the existence of the EU AI Act during onboarding.
- All employees working with AI must be familiar with this policy and complete relevant training.
- A dedicated budget line for AI development and training will be included in the 2026 budget.
- AI shall be addressed in the company's strategic business plan.

ETHICAL PRINCIPLES

GUIDELINES FOR AI USE

- AI-generated content must always be labelled and presented as AI-generated.

- AI may support but must never replace critical decision-making within the company.

- All AI use shall be guided by fairness, transparency, accountability, and integrity.

- Systems must be designed to counteract bias and discrimination.

DATA PROTECTION AND SECURITY

SECURITY MEASURES

- Personal data must not be processed in generative AI systems without a legal basis and appropriate security measures.

- AI systems may not transfer sensitive data to third countries unless GDPR requirements are met.

- Procedures are in place to protect against data leaks, intrusions, and unauthorised access.

- Users must follow the company's IT security policy when handling AI-generated data.

- In the event of an incident, the CEO, IT Manager, HR, or immediate supervisor must be contacted immediately.

USE AND LIMITATIONS

PERMITTED AND PROHIBITED AI TOOLS

- Only AI tools approved by the CEO / IT department may be used.
- AI tools lacking documented security or data protection are prohibited.

PERMITTED AND PROHIBITED DATA

- Business-critical and sensitive company information must not be processed by generative AI.
- Personally identifiable information (PII) may not be used in AI systems without explicit permission.

QUALITY ASSURANCE

- AI-generated output must be reviewed and verified by a responsible person/ manager before use.

RESPONSIBILITY AND MONITORING

DIVISION OF RESPONSIBILITY

- The CEO is responsible for ensuring the policy is followed, evaluated, and updated.
- Users of AI systems are responsible for complying with this policy.
- The IT department is responsible for security measures and technical controls.

TRAINING AND COMPETENCE DEVELOPMENT

AI COMPETENCE REQUIREMENTS

- All direct users of generative AI must complete basic training in AI, including its opportunities and risks.

This policy shall be regularly updated to align with technological developments and current legal requirements.

EWES GROUP

EWES AB
Lundavägen 53
SE-333 71 Bredaryd, Sweden
+46 (0)370 867 00