Sistema Qualità
Sistema di Gestione
Ambientale
ISO 9001
ISO 14001
www.dekra-seal.com
DEKRA certificato

OLAB S.r.l.
Via Cavallera, 2
25030, Torbole Casaglia (BS) - Italy
Tel. +39 030 2159411

C.C.I.A.A. 309654
C.F. 02963700170 **P. IVA** IT 02963700170
Registro Società Tribunale BS 38321
Cap. Soc. 1.820.000,00 Euro i.v.
www.olab.it | olab@olab.it

MODEL FOR ORGANIZATION, MANAGEMENT AND CONTROL

GLOBAL POLICY

FOR THE USE OF ARTIFICIAL INTELLIGENCE (AI)

AND SPECIAL SECTION OF THE ORGANIZATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE No. 231/2001

Approved by resolution of the Board of Directors on December [-], 2025

INDICE

1. FOREWORD AND STRATEGIC CONTEXT

This Corporate Policy for the Use of Artificial Intelligence (hereinafter the "AI Policy") is adopted by OLAB (the "Company") as a tool for the responsible governance of technological innovation, within an industrial context characterized by high requirements in terms of reliability, safety, operational continuity and manufacturer responsibility.
The Company is a leading player in the fluid control and sustainable refrigeration sectors and is directly engaged, with passion and continuous commitment, in the design, manufacturing and marketing of mechanical and electromechanical components intended for industrial and retail applications, where design, production or control errors may generate significant consequences in terms of safety, civil and criminal liability, and corporate reputation.
Within this context, Artificial Intelligence represents an opportunity for efficiency enhancement and decision-making support, but also a source of new technological, organizational and legal risks, which must be adequately addressed through clear rules, appropriate controls and clearly defined responsibilities.

---

2. PURPOSE, LEGAL VALUE AND SCOPE OF APPLICATION

2.1 Purposes

This AI Policy pursues the following objectives:

- to ensure the use of Artificial Intelligence in compliance with applicable laws and regulations;
- to safeguard the safety of products, processes and workers;
- to preserve human oversight over relevant technical decisions;
- to protect the Company's informational, technological and industrial assets;
- to prevent risks of administrative liability pursuant to Legislative Decree No. 231/2001.

2.2 Legal Value

This Policy constitutes a binding internal regulation and supplements the Code of Ethics, the 231 Model, the Quality Management System, the Risk Assessment Document (DVR), as well as the IT and cybersecurity policies.

2.3 Subjective and Objective Scope

This AI Policy applies to employees, executives, directors, collaborators, consultants and suppliers operating on behalf of the Company..

3. REGULATORY FRAMEWORK

This AI Policy is adopted within the framework of the following regulatory measures:

- Legislative Decree No. 231/2001;
- Regulation (EU) 2016/679 (GDPR);
- Regulation (EU) 2024/1689 – the European Union Artificial Intelligence Act, also known as the EU AI Act or AI Act – in force as of 1 August 2024;
- legislation on product safety and manufacturer's liability;
- general and sector-specific legislation on occupational health and safety;
- general and sector-specific legislation on trade secrets and competition;
- general and sector-specific legislation on cybersecurity;

---

4. DEFINITIONS AND CLASSIFICATION OF AI SYSTEMS

4.1 Definitions

For the purposes of this AI Policy, the following operational definitions shall apply. These definitions are drafted in order to ensure interpretative clarity and uniform application within the corporate organization:

- **Artificial Intelligence (AI):** any software, hardware or combined system, developed or used by the Company or by Users, capable of processing data, information or signals and generating outputs such as predictions, recommendations, analyses, classifications or content, with a level of partial or assisted autonomy, based on algorithmic, statistical or machine-learning models.

- **Generative AI:** Artificial Intelligence systems designed to generate new content (texts, images, code, models, conceptual schemes) based on inputs provided by the user, including chatbots, virtual assistants and design support tools.

- **Authorized AI System:** an Artificial Intelligence system that has been subject to a prior technical, organizational, cybersecurity and regulatory compliance assessment, and has been formally approved by the Company in accordance with the internal authorization procedure.

- **User:** any individual or entity who, in any capacity (employee, executive, director, consultant or supplier), uses AI systems within, or for purposes related to, the Company's activities.

- **Confidential Industrial Data:** the set of the Company's technical, technological, production and commercial information, including, by way of example and without limitation: technical drawings, CAD models, electrical diagrams, bills of materials, design parameters, testing parameters, production processes, product specifications, know-how and strategic information.

4.2 Classification of AI Systems Based on Risk

In order to ensure a conscious and proportionate use of Artificial Intelligence, the Company adopts an internal classification of AI systems based on the level of potential risk associated with their use, taking into account the impact on business processes, product safety and manufacturer liability.

a) Low-Risk AI Systems
This category includes AI systems used for administrative, documentary or informational support activities that do not directly affect technical, production or safety-related decisions. Such systems may be used, subject to prior explicit authorization, in compliance with this AI Policy and the Company's IT policies.

b) Medium-Risk AI Systems
This category includes AI systems used to support technical, production or organizational activities, including conceptual design support, production data analysis, predictive maintenance and qualitative trend analysis. The use of such systems always requires qualified human supervision and validation.

c) High-Risk AI Systems
This category includes AI systems that, even potentially, may impact product safety, worker or customer safety, regulatory compliance, CE marking or manufacturer liability. Such systems may never operate autonomously and are permitted exclusively as informational support tools, subject to enhanced authorization and continuous monitoring.

---

5. GENERAL PRINCIPLES FOR THE USE OF ARTIFICIAL INTELLIGENCE

This Chapter defines the general and non-derogable principles governing the use of Artificial Intelligence within the Company. Such principles constitute the ethical, technical and legal foundation of the AI Policy and shall guide every decision, operational choice and conduct of Users.

5.1 Principle of Human Oversight and Precedence of Human Control

The Company acknowledges that Artificial Intelligence constitutes a tool to support human activity and may in no circumstances replace human judgment, expertise, responsibility and discretion.

Any use of AI shall be designed and managed in such a way as to ensure the presence of effective, informed and qualified human oversight, in particular with regard to processes affecting design, manufacturing, product safety and regulatory compliance.

It is expressly prohibited to delegate to AI systems any autonomous or automated decisions that produce significant legal, technical or organizational effects.

5.2 Principle of Responsibility and Attribution of Decisions

Any activity carried out with the support of AI systems shall always be attributable to one or more clearly identified natural persons, who retain full responsibility for the decisions taken and for the outputs generated.

The use of AI shall in no way exempt the User, the relevant functional manager or the Company from any civil, criminal, administrative or disciplinary liability arising from errors, omissions or violations.

5.3 Principle of Traceability and Verifiability

The use of AI systems shall be organized in such a way as to ensure the traceability of the activities performed, the inputs provided, the outputs generated and the decisions adopted on the basis of such outputs. Traceability constitutes an essential requirement for:

- internal verification activities;
- audit activities;
- compliance with oversight and control obligations pursuant to Legislative Decree No. 231/2001;
- the management of any disputes, investigations or inspections.

5.4 Principle of Proportionality and Industrial Precaution

The adoption and use of Artificial Intelligence shall be proportionate to the complexity, criticality and risk level of the process involved.

In industrial processes characterized by potentially significant impacts on product safety, worker safety or customer safety, the Company applies an enhanced precautionary principle, limiting the use of AI to informational and analytical support functions.

5.5 Principle of Product and Process Safety

The safety of mechanical and electromechanical products constitutes a primary and non-negotiable value for the Company.

The use of Artificial Intelligence may in no circumstances compromise, reduce or circumvent the requirements of safety, reliability, quality and regulatory compliance applicable to products and production processes.

Any output generated by AI systems that affects, even indirectly, safety-related aspects shall be subject to qualified technical verification.

5.6 Principle of Regulatory and Legal Compliance

The use of Artificial Intelligence shall take place in compliance with all applicable laws and regulations, including those relating to:

- product safety and manufacturer liability;
- occupational health and safety;
- personal data protection;
- trade secrets and competition;
- administrative liability of legal entities pursuant to Legislative Decree No. 231/2001.

Any use of AI involving interpretative uncertainties or regulatory risk profiles shall be subject to prior assessment by the competent corporate functions.

5.7 Principle of Protection of Informational and Industrial Assets

The Company recognizes and duly safeguards the strategic value of its informational, technical and industrial assets.

The use of Artificial Intelligence shall be structured in such a manner as to **prevent the disclosure, loss or improper use of corporate data, information and know-how, through the adoption of appropriate organizational and technical measures.**

---

6. AI AND CORPORATE INDUSTRIAL PROCESSES

This Chapter specifically regulates the use of Artificial Intelligence within the Company's main industrial and support processes, with the aim of ensuring that such use is consistent with the principles of safety, human oversight, responsibility and regulatory compliance.

6.1 AI and Product and Component Design

Artificial Intelligence may be used as a support tool in the product or component design phase exclusively for purposes of preliminary analysis, conceptual simulation, design consistency checks and support in identifying alternative solutions.
In this context:

- AI may **not be used for the autonomous design of components or assemblies;**
- any output generated by AI systems shall be verified, validated and approved by qualified technical personnel;
- the obligation to comply with applicable technical regulations, product specifications and the Company's design procedures shall remain fully in force.

It is expressly **prohibited to use AI systems to replace the technical validation process, design reviews or safety assessments.**

6.2 AI and Product Industrialization

During the industrialization phase, Artificial Intelligence may be used to support:

- the analysis of production processes;
- the optimization of operational flows;
- the preliminary evaluation of alternative process solutions.

Under no circumstances may AI replace industrialization decisions, which shall remain the exclusive responsibility of the competent senior corporate functions.

6.3 AI and Production

Within the production process, Artificial Intelligence may be used for:

- the analysis of production data;
- the identification of anomalies or inefficiencies;
- support to production planning activities.

It is prohibited to entrust AI systems with the direct and autonomous control of machinery, equipment or production lines in the absence of adequate safety safeguards and effective human supervision.

6.4 AI and Quality, Testing and Certifications

Artificial Intelligence may support quality and testing activities through the analysis of historical data, trend detection and support to document management.

Under no circumstances may AI:

- replace mandatory physical tests;
- automatically validate testing results;
- be used as the sole tool to certify product conformity;
- autonomously affect CE marking or the technical documentation file.

6.5 AI and Maintenance

Artificial Intelligence may be used for predictive and preventive maintenance purposes, in order to support the identification of potential failures or critical issues.

Operational decisions relating to maintenance interventions shall **in any case remain the responsibility of qualified technical personnel.**

6.6 AI and Technical Data Management

The use of Artificial Intelligence for the analysis and management of technical data shall take place in compliance with the Company's IT policies and the security measures adopted by the Company.

It is prohibited to use AI systems that result in the uncontrolled disclosure of technical data, drawings or confidential information.

6.7 AI, Information Systems and Cybersecurity

Each AI system shall be subject to a prior cybersecurity assessment. The integration of Artificial Intelligence into the Company's information systems shall ensure:

- segregation of access rights;
- traceability of operations;
- protection against unauthorized access;
- auditability.

---

7. PERMITTED, RESTRICTED AND PROHIBITED AREAS OF USE OF AI

This Chapter clearly and exhaustively identifies the areas of use of Artificial Intelligence that are permitted, subject to restrictions or prohibited within the Company, with the aim of preventing improper use, reducing operational risk and ensuring compliance with the principles of safety, human oversight and responsibility.

7.1 Permitted Areas of Use

The use of AI systems is permitted, subject to prior authorization and in compliance with this AI Policy, for the following purposes:

- **Documentary and informational support:** drafting of internal document outlines, regulatory summaries, and support in the preparation of procedures and manuals, it being understood that the final version shall always be reviewed and approved by competent personnel.

- **Analysis of historical data:** analysis of production, quality, maintenance and logistics data in order to identify trends, correlations and potential areas for improvement.

- **Conceptual design support:** use of AI for technical brainstorming activities, preliminary analysis of design solutions and non-binding conceptual assessments.

- **Predictive maintenance:** support in identifying potential failures or critical issues, without replacing the operational decisions of qualified technical personnel.

- **Planning support:** analysis of production scenarios, resource planning and support to organizational decision-making.

7.2 Restricted Areas of Use

Uses of AI that affect, even indirectly, significant technical or industrial processes are subject to specific restrictions and enhanced controls.

The following fall within this category:

- **Technical design:** AI may be used solely as an informational support tool; any output shall be subject to qualified technical verification and validation.
- **Quality and testing:** AI may support the analysis of testing data, but may not validate results nor certify product conformity.
- **Production:** AI may analyze process data, but may not autonomously control machinery or production lines.
- **Technical data management:** the use of AI is permitted only on authorized systems and exclusively with adequately protected data.

For all such areas, continuous supervision by qualified personnel is mandatory.

7.3 Prohibited Areas of Use

It is expressly and non-derogably prohibited to use AI systems for:

- the autonomous design of safety-critical mechanical or electromechanical components;
- replacing mandatory physical tests, required trials or prescribed testing activities;
- automatically validating the regulatory compliance of products;
- autonomously affecting CE marking or the technical documentation file;
- circumventing or evading quality, safety or compliance controls;
- **uploading, inputting or sharing any corporate documentation, and in particular technical drawings, CAD models, technical or test results, testing reports, inspection records and CE documentation;**
- using AI for disciplinary assessments, performance evaluations or personnel selection;
- using AI in a manner contrary to the Code of Ethics or applicable laws and regulations.

7.4 Consequences of Violations

Any use of Artificial Intelligence in violation of this Chapter shall constitute a serious breach of the AI Policy and shall result in the application of the applicable disciplinary sanctions, without prejudice to any further civil, criminal or administrative liability.

---

8. DATA PROTECTION, KNOW-HOW AND CYBERSECURITY

This Chapter governs the measures and rules aimed at protecting personal data, industrial data and the Company's know-how in the context of the use of Artificial Intelligence, as well as the cybersecurity safeguards required to prevent risks of loss, unauthorized disclosure or compromise of information.

8.1 Protection of Personal Data

The use of AI systems involving the processing of personal data shall take place in full compliance with applicable personal data protection regulations, including Regulation (EU) 2016/679 (GDPR), as well as the Company's internal policies and procedures.

In particular:

- it is prohibited to input personal data into AI systems where such data are not necessary for the purposes pursued;
- where possible, data shall be anonymized or pseudonymized in advance;
- any use of AI involving new or high-risk processing activities shall be subject to a prior privacy assessment, including, where applicable, a Data Protection Impact Assessment (DPIA);
- roles and responsibilities in relation to data protection shall be clearly identified.

8.2 Protection of Know-How and Trade Secrets

The Company acknowledges the strategic value of its technical, industrial and documentary assets and adopts **an absolute prohibition principle on the uploading of corporate documentation to Artificial Intelligence systems that have not been expressly authorized.**

It is **expressly, generally and non-derogably prohibited** to upload, input or share, even partially, on any AI system (including cloud-based systems, external platforms, chatbots and generative AI tools) the following:

- technical drawings, CAD models, mechanical and electromechanical diagrams;
- results of technical tests, laboratory tests, testing activities, functional or safety verifications;
- test reports, testing records, reliability analyses;
- design parameters, technical specifications, bills of materials;
- technical documentation files and documentation relating to CE marking;
- production procedures, industrial processes and the Company's know-how;
- any other confidential or non-public corporate documentation.

This prohibition shall **apply regardless of:**

- the document format (text, image, CAD file, screenshot, photograph);
- the device used (corporate or personal);
- the declared purpose of use.

It is also prohibited to use AI systems that provide for the use of uploaded data for training, learning or model improvement purposes, even in aggregated form.

Any breach of this prohibition shall be deemed a **serious violation of the AI Policy,** the Code of Ethics and confidentiality obligations, and shall expose the responsible party to disciplinary sanctions as well as any further liabilities provided for by applicable law.

8.3 Cybersecurity and System Protection

The adoption and use of AI systems shall take place in compliance with the Company's cybersecurity policies and recognized best practices in the field of cybersecurity.

In particular:

- AI systems shall ensure adequate levels of security, authentication and access control;
- protective measures shall be implemented to prevent unauthorized access, data loss and cyberattacks;
- the integration of AI into the Company's information systems shall be subject to prior assessment by the IT function;
- the traceability of operations and the possibility of audit shall be ensured.

8.4 Incident Management and Reporting

Any security incidents, data breaches or improper uses of Artificial Intelligence shall be promptly reported in accordance with the Company's internal procedures, in order to allow the adoption of appropriate corrective and preventive measures.

Failure to report incidents or violations shall constitute a breach of this AI Policy.

---

9. INTERNAL GOVERNANCE OF ARTIFICIAL INTELLIGENCE

This Chapter defines the internal governance framework for Artificial Intelligence adopted by the Company, identifying roles, responsibilities, decision-making processes and control mechanisms aimed at ensuring the compliant, secure and traceable use of AI, in alignment with the Organization, Management and Control Model pursuant to Legislative Decree No. 231/2001.

9.1 Governance Principles

The governance of Artificial Intelligence is based on the following principles:

- clear allocation of roles and responsibilities;
- segregation of decision-making and control functions;
- continuous oversight and human supervision;
- integration with the internal control system and the 231 Model;
- documentation and traceability of decisions.

9.2 Bodies and Functions Involved

Within the framework of AI governance, the following bodies and functions are involved, each within their respective areas of responsibility:

- **Board of Directors:** approves this AI Policy and ensures its adequacy with respect to the Company's strategy and risk profile.

- **Senior Management**: ensures the operational implementation of the AI Policy and the compliant integration of AI into corporate processes.

- **Compliance / 231 Model Officer**: oversees regulatory risk and the corporate administrative liability profiles associated with the use of AI.

- **Supervisory Body (SB)**: monitors the effective implementation of the AI Policy and receives the envisaged information flows.

- **IT and Cybersecurity Function**: assesses AI systems from a technical and cybersecurity perspective.

- **Functional Managers (Technical, Production, Quality, etc.):** ensure that AI is used within their respective areas in compliance with this AI Policy.

9.3 AI Use Authorization Process

The use of Artificial Intelligence systems is permitted exclusively subject to prior formal authorization, in accordance with the Company's internal procedures.

As a general rule, the authorization process includes:

- a reasoned request submitted by the relevant corporate function;
- technical and cybersecurity assessment;
- assessment of regulatory risks and risks under Legislative Decree No. 231/2001;
- where applicable, involvement of the Supervisory Body (SB);
- registration of the authorized AI system.

9.4 Register of AI Systems

The Company establishes and maintains an up-to-date register of authorized Artificial Intelligence systems, containing at least the following information:

- description of the system;
- intended purpose of use;
- risk level;
- involved corporate functions;
- date of authorization and review.

9.5 Monitoring and Audit

The use of AI systems is subject to periodic monitoring and, where necessary, internal audits. Monitoring activities are aimed at:

- verifying compliance with this Policy;
- identifying improper or unauthorized uses;
- assessing the adequacy of control mechanisms.

9.6 Management of Non-Compliance

Any non-compliance, violations or improper use of AI shall be promptly managed through the adoption of corrective and preventive measures, in coordination with the competent corporate functions and, where applicable, with the Supervisory Body.

---

10. TRAINING, RESPONSIBILITIES AND DISCIPLINARY SYSTEM

This Chapter governs training obligations, individual responsibilities and the disciplinary system related to the use of Artificial Intelligence, in order to ensure the effective implementation of this Policy and its integration into the internal control system and the Organization, Management and Control Model pursuant to Legislative Decree No. 231/2001.

10.1 Training and Awareness

The Company recognizes that a proper understanding of the risks and opportunities associated with Artificial Intelligence is an essential prerequisite for the conscious and compliant use of AI tools.

To this end, the Company ensures:

- mandatory periodic training programs for employees and executives involved in the use of AI;
- specific training modules for technical, production, quality, IT and compliance functions;
- awareness-raising activities on legal, organizational and security risks related to improper use of AI;
- training updates in the event of relevant regulatory, technological or organizational changes.

Participation in training activities constitutes a work obligation and shall be adequately tracked.

10.2 Individual Responsibilities

Each recipient of this AI Policy is required to:

- be familiar with and comply with the provisions of this AI Policy;
- use exclusively authorized AI systems;
- comply with corporate procedures and instructions issued by the competent functions;
- cooperate in monitoring and audit activities;
- promptly report any anomalies, violations or improper uses of AI.

Violation of the obligations above entails individual responsibility and may not be justified by the use of AI tools or reliance on automatically generated outputs.

10.3 Disciplinary System

Failure to comply with this Policy constitutes a breach of contractual obligations and may result in the application of disciplinary sanctions provided for by the Company's disciplinary system and the 231 Model, in proportion to the seriousness of the violation.

By way of example, disciplinary violations may include:

- use of unauthorized AI systems;
- breach of the prohibitions set forth in the AI Policy;
- failure to report incidents or improper uses;
- input of confidential or protected data into AI systems;
- circumvention of prescribed controls.

Any further civil, criminal or administrative liability provided for by law remains unaffected.

---

11. INTEGRATION INTO THE ORGANIZATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE NO. 231/2001

This Chapter governs the integration of the Corporate Policy for the Use of Artificial Intelligence into the Organization, Management and Control Model adopted by the Company pursuant to Legislative Decree No. 231/2001, as a Special Section aimed at preventing risks of corporate administrative liability related to the use of AI.

11.1 Role of the AI Policy within the 231 System

This AI Policy constitutes an integral part of the 231 Model and, together with the Code of Ethics, the disciplinary system and corporate procedures, contributes to preventing the commission of predicate offences potentially related to the use of Artificial Intelligence.

The adoption and effective implementation of the AI Policy represent appropriate organizational safeguards demonstrating the Company's commitment to consciously governing emerging risks arising from technological innovation.

11.2 Mapping of Sensitive Processes

With regard to the use of AI, the following are identified as sensitive processes for the purposes of Legislative Decree No. 231/2001, in particular:

design and development of mechanical and electromechanical components;
industrialization and production;
quality, testing, certification and CE marking;
management of technical and industrial data;
information systems and cybersecurity;
management of technology suppliers.

These processes are subject to specific control and monitoring safeguards.

11.3 Relevant Predicate Offences

Improper or non-compliant use of Artificial Intelligence may expose the Company to the risk of committing, inter alia, the following predicate offences:

- negligent offences relating to occupational health and safety (Article 25-septies);
- negligent offences related to product safety and manufacturer liability;
- computer crimes and unlawful data processing (Article 24-bis);
- offences against industry and trade;
- violation of trade secrets.

11.4 Specific Control Safeguards

In order to prevent the risks referred to in this Chapter, the Company adopts the following safeguards:

- clear regulation of AI use through this AI Policy;
- formal authorization and registration process for AI systems;
- segregation of roles between users, authorizing bodies and control functions;
- mandatory human technical validation of AI outputs;
- periodic monitoring and audit activities;
- mandatory staff training;
- effective disciplinary system.

11.5 Information Flows to the Supervisory Body

The following shall be promptly reported to the Supervisory Body:
- unauthorized or non-compliant uses of AI;
- significant incidents or anomalies;
- violations of the AI Policy;
- outcomes of internal audits relating to AI usage.

The Supervisory Body assesses the reports received and, where necessary, proposes the adoption of corrective measures.

11.6 Coordination with Other Control Instruments

This Policy is coordinated with:

- the Code of Ethics;
- the Risk Assessment Document (DVR);
- the quality management system;
- IT and cybersecurity procedures;
- the disciplinary system.

Such coordination ensures an integrated approach to AI risk management.

---

12. OPERATIONAL ANNEXES

Annex 1 – Communication to Employees
Annex 2 – Employee Acknowledgment and Acceptance