CORPORATE POLICY FOR THE DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE AGENTS

Política Corporativa Versión 1.0

OBJECTIVE

The objective of this policy is to define a regulatory framework for the design, development, deployment, and use of artificial intelligence agents in the organization, ensuring that such solutions:

- Comply with ethical and legal principles.
- Protect the privacy and security of information.
- Are technically robust, transparent, and auditable.
- Promote the efficiency and quality of internal processes.
- Include human oversight and risk management mechanisms.

This policy aims to ensure that the use of AI agents contributes responsibly and sustainably to Molymet's digital transformation, strengthening the trust of users, employees, customers, and other stakeholders.

The purpose of this policy is to establish the principles, guidelines, and standards that guide the development, implementation, and use of artificial intelligence (AI) agents within Molymet. This policy seeks to ensure that such agents are designed and operated in an ethical, secure, transparent manner that is aligned with the company's strategic objectives.

It also aims to promote responsible innovation, guaranteeing data protection, non-discrimination, the traceability of automated decisions, and adequate human supervision.

SCOPE

All employees of Molymet and its subsidiaries. This policy also applies to members of the company's Board of Directors. This policy applies to all internal development teams, external suppliers, and users involved in the design or use of AI-based solutions.

This policy covers both internally developed AI solutions and those contracted to third parties, including platforms based on generative language models (LLMs), virtual assistants, recommendation systems, cognitive automation, among others.

POLITICAL OWNER

Vice President of Finance.

DESCRIPTION

GUIDING PRINCIPLES OF THE POLICY

1. Ethics and Responsibility

AI agents must be developed and used ethically, respecting fundamental rights, avoiding bias and discrimination, and promoting human well-being. Every automated action must have a clearly defined human responsible party.

2. Transparency

AI agents must operate in a manner that is understandable to users, allowing them to understand how and why automated decisions are made. The traceability of the training process, decisions, and data used must be guaranteed.

3. Privacy and Data Protection

AI development must strictly comply with current regulations on privacy and personal data protection. Measures must be implemented to anonymize, encrypt, or minimize the use of sensitive data whenever possible.

4. Security and Robustness

AI agents must be designed with high cybersecurity standards, mitigating risks of manipulation, misuse, or uncontrolled failures. Mechanisms must be included for detecting and responding to incidents arising from the operation of AI.

5. Human Oversight

All AI solutions must include human control or validation points, especially in critical processes or those with a significant impact on people, critical processes, or strategic decisions. Human oversight must be effective, informed, and have a real capacity for intervention.

6. Inclusion and Non-Discrimination

The models and data used must not reproduce or amplify social, gender, racial, or economic biases. Regular testing must be carried out to ensure fairness in the results generated by AI.

7. Responsible Innovation

The use of AI to improve processes, productivity, and services will be promoted, encouraging innovation, but always within a framework of technological responsibility and in line with corporate strategy.

8. Regulatory Compliance

All AI solutions must comply with applicable local and international legislation, as well as the company's internal guidelines on ethics, information security, and compliance.

DEVELOPMENT OF AI AGENTS

All development of artificial intelligence agents must follow structured steps to ensure their alignment with this policy, their usefulness to the business, and their ethical and safe operation. The following are the minimum aspects that must be considered in each initiative:

1. Definition of the Agent's Scope and Purpose
   - The functional objective of the AI agent.
   - The problem or need it seeks to solve.
   - The scope of its capabilities, operational limits, and use cases.
   - The level of autonomy allowed and the conditions for human oversight

2. Model and Technology Selection
   The following must be specified:
   - The type of AI model used (e.g., language model, classification, recommendation, etc.).
   - Whether it is an in-house development, use of a pre-trained model, or a third-party solution.

- The tools, platforms, and technological frameworks adopted (e.g., TensorFlow, Azure OpenAI, Vertex AI, etc.).
- Technical and ethical criteria underlying the choice.

3. Data Set Definition and Management
   Every AI agent must be supported by a properly managed data set. The following must be documented:
   - The origin of the data used for training.
   - The quality, representativeness, and possible bias of the data.
   - Update cycles and version control of the data set.

4. Assignment of Responsibility
   A formal person in charge of the AI agent must be assigned, who will be:
   - Responsible for leading the development, implementation, and monitoring of the agent.
   - The point of contact for internal or external audits.
   - Responsible for its documentation, continuous improvements, and eventual removal or replacement.

5. Mandatory Participation of Corporate IT Management
   Corporate IT Management must be involved in all AI projects, with the aim of:
   - Ensuring compliance with this policy and other internal regulations.
   - Validating the technical architecture and secure integration with existing systems.
   - Assessing security risks, operational continuity, and information leaks.
   - Defining scalability and technology governance criteria.

6. Risk Assessment and Security Controls
   - Every project must undergo a risk assessment covering cybersecurity, data protection, and operational continuity.
   - Specific controls must be defined to prevent misuse, information leaks, or operation outside authorized parameters

7. Supervision, Logging, and Traceability
   - Every agent must have mechanisms for monitoring performance, activity logs, and auditing key decisions.
   - There must be a centralized registry of AI agents in production, including their versions, responsible parties, and impact assessments

8. Ethical Review and Validation (if applicable)
   - In cases of significant impact (e.g., decisions affecting people, critical operations, or regulations), development must be approved by the VP of the area.

USE OF ARTIFICIAL INTELLIGENCE TOOLS

1. It is strictly prohibited to **upload, share, or process documents**, **data, or information** owned by Molymet in public or external Artificial Intelligence tools without express authorization.

2. For interactions with non-corporate AI, other than uploading, sharing, or processing documents, you should always act under the principle that information shared with the AI tool is accessed by third parties.

3. In online meetings where strategic and/or confidential topics are discussed, the participation of BOTs or external Note Agents is prohibited. Only TEAMS Premium – COPILOT 365, or similar versions managed by Molymet, are permitted.

4. The Generative Artificial Intelligence (LLM) approved for document processing at Molymet is COPILOT 365. This licensing is managed directly by Corporate IT and Digital Transformation Management. Assigning this license to users requires approval from the VP of the area.

5. Any specific need to use AI in business processes, whether it be a request for COPILOT 365 or another application, must be managed through the **Service Desk**, which will refer the matter to the relevant departments for authorization.

SANCTIONS

Failure to comply with this policy may result in disciplinary action in accordance with Molymet's internal regulations.

PROVISIONS FOR MONITORING COMPLIANCE WITH THE POLICY

Those responsible for compliance with this policy are:

1. Corporate IT and Digital Transformation Manager
2. Head of Information Security
3. AI Agent Developers
4. AI Agent Users
5. Corporate VP of Compliance and Risk
6. Molymet Employees

RESPONSIBILITIES

Directory:	- Approval of the policy.
Corporate IT & DX Management	- Implement the policy. - Update the policy. - Comply with defined controls.
Corporate Vice President of Compliance and Risk	- Supervise compliance with the policy.
All employees of Molymet and its subsidiaries	- Comply with policy guidelines

VALIDITY

VALIDITY:
From March 2026.

REVIEW:
Annual.

REFERENCE TO OTHER REGULATORY DOCUMENTS

- Corporate Information Security and Cybersecurity Policy.
- Corporate Data Governance and Protection Policy.
- Corporate Policy on Information Sharing.
- General Data Protection Regulation (GDPR).
- ISO/IEC 27001: International standard for information security management.
- ISO/IEC 23894: Artificial intelligence risk management.
- NIST AI Risk Management Framework (AI RMF): Framework for identifying, assessing, and mitigating risks associated with AI systems.
- OECD and European Union AI ethics guidelines: Principles on responsible use, transparency, fairness, and human oversight.

POLICY COMMUNICATION CHANNELS

Platform for Policy and Procedure Document Management (GDPP)

This policy was approved by the Board of Directors of Molibdenos y Metales S.A. at Meeting No. 1043, held on March 23, 2026, and has been in effect since that date.

P.P.

EDGAR PAPE ARELLANO
Chief Executive Officer
Molibdenos y Metales S.A.

MOLYMET®