CORPORATE POLICY

GOVERNANCE AND DATA PROTECTION

Corporate Policy Version 1.0

OBJECTIVE

This policy establishes general guidelines for the management and protection of information assets and personal data across all units and processes of the organization, ensuring compliance with applicable legislation.

It aims to guarantee proper governance, confidentiality, integrity, and protection of corporate information assets, including the personal data of individuals, promoting responsible information management that supports operational continuity, regulatory compliance, and the trust of all stakeholders.

The Data **Governance and Protection Policy** and the **Information Security and Cybersecurity Policy** have the essential objective of contributing, through their specific provisions, to safeguarding and promoting an organizational culture focused on protecting information in all its forms. Essentially, the link between these two policies allows for compliance with the principles of privacy and confidentiality, complemented by cybersecurity action guidelines.

- Ensures the protection of sensitive and personal data of employees, customers, suppliers, and other stakeholders.
- Comply with applicable legal and regulatory requirements regarding data protection.
- Establishes a data governance framework that facilitates decision-making based on reliable and accurate information.
- Promotes an organizational culture focused on data protection and ethical information management.

SCOPE

This policy applies to all employees of Molymet and its subsidiaries. It also applies to members of the company's Board of Directors, as well as to third parties who have access to information assets, including personal data processed by the organization. It extends to all processes involving the collection, storage, processing, transmission, and disposal of information assets and data in any format, regardless of the medium used, and to all companies or suppliers that directly or indirectly manage the organization's data.

OWNER

Vice Presidency of Finance.

DESCRIPTION

GUIDING PRINCIPLES OF THE POLICY

To ensure the protection of information and compliance with current regulations, the following principles are established:

1. Data Governance: Information must be managed in a structured manner, ensuring quality, traceability, and availability for decision-making. A data governance team will be defined, with clear roles and responsibilities, and an inventory of information assets (classified according to sensitivity and use) will be maintained.

2. Compliance with personal data regulations: The processing of personal data must be carried out in accordance with the following principles:
   (i) Lawfulness and loyalty, acting legally and fairly, always respecting the rights of the holder.

   (ii) Purpose, collecting and using the data only for specific, lawful, and previously informed purposes.

   (iii) Proportionality, limiting the processing to the data strictly necessary and keeping them only for the necessary time.

   (iv) Quality, ensuring that the data is accurate, complete, up-to-date, and relevant.

   (v) Responsibility, complying with current regulations and guaranteeing proper data handling.

   (vi) Security, protecting data against unauthorized access, loss, or leakage.

   (vii) Transparency and information, providing the data subject with clear, free, and permanent access to information about the processing of their data.

   (viii) Confidentiality, keeping the data secret even after the relationship with the data subject has ended.

3. Confidentiality:
   - Data (corporate and personal) must be protected against unauthorized access or disclosure.
   - The acquisition, collection, or transfer of data from illegitimate sources or without guarantees of origin and protection is prohibited.

4. Integrity:
   - The information must be accurate, consistent, and protected against unauthorized modifications.

5. Transparency and Information:

- At all times, data subjects must be informed clearly, precisely, and accessibly about the purpose of the processing, the recipients of the data, the legal basis and the retention period.
- Whenever required by applicable law, your express consent will be obtained for its collection and/or processing.

6. Shared and Proactive Responsibility:
   - The entire organization is responsible for protecting and properly managing the information assets and personal data that they collect or store.
   - The necessary technical and organizational measures will be implemented for proper treatment and protection, and the effectiveness of these measures will be reviewed periodically.

7. Rights of the Holders:
   - Data subjects may exercise their rights of access, rectification, erasure, objection, restriction of processing, and data portability, in accordance with applicable law.
   - Internal procedures will be established to ensure effective handling of data subject requests within the legally established timeframes.

CONTROLS

Data Governance:

- Create a team responsible for data governance.
- Define information assets.
- Document and maintain an inventory of information assets, classifying them according to their sensitivity level and use.
- Define clear roles and responsibilities for information management.
- Establish clear processes for the collection, storage, processing, archiving, and secure disposal of data.
- Ensure that data is not retained longer than necessary, in accordance with legal regulations.
- Implement guidelines regarding artificial intelligence in data governance.

Personal Data Protection:

- Regulatory Compliance: Mechanisms must be implemented to ensure compliance with Chilean Law 19.628 on the protection of personal data, the General Data Protection Regulation (GDPR) – where applicable, as well as any applicable local regulations.
- Consent and Purpose: Where required by law, the express consent of data subjects must be obtained, and they must be informed about the purpose of the processing and use of their data.

Information Security (corporate and personal data):

- Technical and Organizational Measures: Measures such as encryption, access controls, periodic audits, and incident recovery plans should be adopted.

- Incident Management: An incident management procedure must be established to report, assess, and respond promptly to any security risks or breaches affecting personal or corporate data.
- Cybersecurity: This Policy will be complemented by the existing cybersecurity policy, ensuring comprehensive protection against digital threats.

Hiring of Data Processors
- Before contracting external services that involve access to personal data, it is essential to verify that the respective provider complies with all applicable legal, regulatory, and security requirements.
- Agreements or contracts detailing the data processor's obligations regarding the confidentiality, integrity, and availability of the data must be signed, including liability clauses and security measures aligned with applicable regulations.

Training and Awareness:
- Regular training programs on data protection and information security must be established for all employees and managers, and the same commitment will be required of suppliers and subcontractors.
- These programs will include responsibilities for safeguarding information, as well as the importance of complying with applicable regulations.

The controls mentioned must be developed through specific documented Procedures and Guidelines and reviewed periodically.

RESPONSIBILITIES

Board:	- Approve the policy.
Corporate IT & DX Management.	- Implement the policy. - Update the policy. - Comply with defined controls.
Corporate Vice Presidency of Compliance and Risk	- Monitor policy compliance.
All employees of Molymet and its subsidiaries	- Comply with policy guidelines.

VALIDITY

VALIDITY:
Effective as of January 2026.

REVIEW:
Annual.

REFERENCE TO OTHERS REGULATORY DOCUMENTS

- Corporate Policy for sharing information.
- Information Security and Cybersecurity Policy.
- General Data Protection Regulation (GDPR).
- Law 21.719 on the regulation and processing of personal data.
- Law 19.628 on the protection of personal data.
- ISO 27001: Information Security Management.

POLICY COMMUNICATION CHANNELS

Platform Documentary Management of Policies and Procedures "(GDPP)"

This policy was approved by the Board of Directors of Molibdenos y Metales S.A. at Meeting No. 1041, held on January 21, 2026, and has been in effect since that date.

P.P.

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

MOLYMET®