CORPORATE POLICY
INFORMATION SECURITY AND CYBERSECURITY

Corporate Policy Version 1.0

OBJECTIVE

Information security is a fundamental pillar for protecting Molymet's digital assets, operational continuity, and reputation. This information security and cybersecurity policy establishes the guidelines, principles, and responsibilities that all employees, contractors, and stakeholders must follow to safeguard information against internal and external threats.

Its purpose is to guarantee confidentiality, integrity, and availability of information, as well as compliance with applicable legal, contractual, and regulatory requirements. The policy covers areas such as the protection of technological systems, access management, prevention of data breaches, cyber defense against incidents, risk management, staff awareness, the appropriate use of technological resources, and resilience against cyberattacks.

In this way, an organizational culture focused on protecting information in all its forms is promoted, ensuring that processes, systems, and people operate within a security framework aligned with Molymet's strategic objectives.

The **Information Security and Cybersecurity policy** is a fundamental pillar in ensuring the effectiveness of the **Data Governance and Protection policy**, as both policies share the essential objective of contributing, through their specific provisions, to the safeguarding and protection of 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.

This Policy applies to

- Protect confidentiality, integrity, and availability of corporate information.
- Manage the risks associated with cyber threats and attacks.
- Promote a cybersecurity culture throughout the organization.
- Comply with applicable laws and regulations.

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 our technological resources and personal data processed by the organization. It extends to all processes involving the collection, storage, processing, transmission, and deletion of information and data assets 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 information protection, cybersecurity, and compliance with current regulations, the following principles are established:

- Confidentiality: Sensitive information should only be accessible to authorized personnel.
- Integrity: Ensuring that data is not altered or manipulated without authorization.
- Availability: Ensuring that systems and data are available for use when needed.

To structure its information security and cybersecurity management, Molymet adopts the **NIST Cybersecurity Framework**, internationally recognized for its comprehensive and flexible approach. This model is based on five key functions that enable the coherent organization of security activities:

- **Identify**: critical assets, risks, and resources.
- **Protect**: through technical controls, policies, and awareness.
- **Detect**: incidents, anomalies, and unauthorized access.
- **Respond**: with action plans for security events.
- **Recover**: by restoring normal operations after an incident.

This structure allows us to proactively manage cyber risks, adapt to changing environments, and continuously strengthen our security posture.

CONTROLS

In accordance with the framework, Molymet and its subsidiaries must have the following specific Information Security controls:

1. IT Infrastructure Security:

   Scope: Protection mechanisms must be implemented on all computing devices used by the organization, including workstations, servers, mobile devices, and network equipment. This includes:

   Antivirus and antimalware: Installation and maintenance of up-to-date solutions that allow for the detection and removal of malicious software.

   Data encryption: Application of encryption to hard drives, mobile devices, and external storage media to protect confidentiality of information.

   Updates and patches: Establishment of a regular process for installing security patches and operating system and application updates to reduce exploitable vulnerabilities

   - **Metrics:**
     - % of PCs with active and up-to-date protection.
     - % of servers with active and up-to-date protection.
     - % of switches with active and up-to-date protection.
     - % of devices with critical patches applied.
     - % of devices with encryption enabled.

2. Network Security:

Scope: The corporate network must be protected using devices and tools that allow for constant monitoring and threat detection. This includes:

- Firewalls, IDS/IPS and UTM systems: Configuration and maintenance of devices that control incoming and outgoing traffic, detect intrusions and block suspicious activity.
- Network segmentation: Separating networks by security levels (e.g., user network, server network, guest network) to limit the lateral movement of threats.
- Continuous monitoring: Implementation of solutions for the collection, analysis, and correlation of security events.

- **Metrics:**
  - Number of network events blocked by security rules.
  - % of networks segmented by criticality.
  - % of IT network monitoring coverage.

3. Access Management:
   Scope: Strict controls must be established to ensure that only authorized personnel access the organization's systems, applications, and data. This includes:
   - Logical access: Use of multi-factor authentication (MFA), secure password management, and assignment of permissions based on the principle of least privilege.
   - Physical access: Control of entry to facilities through access cards, biometrics or other mechanisms, especially in critical areas such as server rooms.
   - Periodic review: Regular audits of accounts and access to detect and eliminate unnecessary or unauthorized access.
   - **Metrics:**
     - % of accounts with multi-factor authentication (MFA) enabled.
     - % of inactive accounts deleted on time.
     - Number of unauthorized accesses detected.

4. Data Management:
   Scope: Information must be managed according to its level of sensitivity and in compliance with current legislation, such as the Personal Data Protection and Processing Act. This implies:
   - - Information classification: Identification and categorization of data (public, internal, confidential, sensitive).
   - - Personal data protection: Implementation of technical and organizational measures to guarantee the privacy and security of personal data.
   - - Role and profile management: Clear definition of responsibilities and access permissions to information according to the user's role.
   - - Regulatory compliance: Ensuring that all data processing activities are aligned with applicable national and international legislation.
   - **Metrics:**
     - • Percentage of systems with applied data classification.
     - • Number of personal data breaches reported.

5. Operational Resilience:

Scope: The organization must be prepared to respond to incidents that affect business continuity. This includes:

- Business Continuity Plans (BCPs): Documentation of procedures to maintain critical operations during disruptions.
- Disaster Recovery Plans (DRPs): Strategies to restore systems and data in the event of serious failures or cyberattacks.
- Periodic testing: Drills and tests of the plans to validate their effectiveness and make continuous improvements.

- **Metrics:**
  - % of critical systems with successfully tested backups.
  - % of operational continuity test compliance.

6. Safe Culture:
   Scope: To foster a cybersecurity-oriented organizational culture through training and awareness programs for all employees. This includes:

   - Ongoing training: Regular programs on topics such as phishing, secure password use, safe browsing, and handling confidential information.
   - Assessments and campaigns: Conducting awareness campaigns, social engineering tests, and surveys to measure cybersecurity maturity levels.

   - **Metrics:**
     - % of employees trained in cybersecurity
     - % of simulated phishing campaign completion (click-through rate, incident reporting).
     - Number of training sessions conducted annually per subsidiary

CREATION OF A CYBERSECURITY CRISIS COMMITTEE

The Cybersecurity Crisis Committee is established as the body responsible for leading the organizational response to large-scale disruptive events that could affect operational continuity, system integrity, and information security at Molymet.

Its function is to coordinate strategic, tactical, and operational actions to mitigate the impact, restore critical operations, and protect the interests of the organization, its employees, clients, and stakeholders.

In the specific context of cybersecurity incidents, the Crisis Committee aims to coordinate incident containment, mitigate its technical and reputational impact, ensure the continuity of critical digital services, and lead institutional communication with internal and external stakeholders.

- Members of the Cybersecurity Crisis Committee:
  1. Corporate IT and Digital Transformation Manager (Committee Leader).
  2. Cybersecurity Manager.
  3. Corporate Communications Manager.
  4. Legal Manager or Corporate Legal Counsel.
  5. Operations Manager (if applicable due to production impact).
  6. Representative from the Corporate Vice Presidency of Compliance and Risk.

7. Other members or technical advisors (depending on the nature of the incident).

The Committee may convene other internal or external leaders or experts when the situation requires it, including representatives from subsidiaries, critical suppliers, or the Human Resources area if the incident warrants it.

- Cybersecurity Crisis Committee Activation Criteria:

  The Cybersecurity Crisis Committee must be activated immediately when a cybersecurity event occurs that meets one or more of the following criteria:

  1. Compromise of critical systems or key infrastructure: Incidents that affect the availability or functionality of systems essential to Molymet's operations (e.g., SAP, OT industrial networks, financial or production systems). Incidents that generate simultaneous or cascading effects in different areas, plants, or subsidiaries of the Molymet group, making them difficult to contain at the local level.
  2. Loss, exposure or theft of sensitive or confidential information: Any leakage, unauthorized access or loss of personal, strategic, commercial, regulatory or third-party data that may compromise the security or image of the company.
  3. Violations of regulations or risk of regulatory sanction: Any event that involves non-compliance with laws or regulations regarding cybersecurity, personal data protection, or contractual standards required by third parties.

- Crisis Committee Activation Process:

  Initial incident detection will be the responsibility of the Cybersecurity or Technology department, through its monitoring systems or internal reports. If the incident meets the criteria outlined above, it must be immediately escalated to the Corporate IT and Digital Transformation Manager, who will have the authority to formally declare a crisis and activate the Committee.

  The meeting will be convened through corporate channels (email and Teams). If any member cannot be contacted immediately, they will be reached by phone or WhatsApp. The Committee must convene within one hour of its activation.

  During the first meeting, specific roles will be assigned, the situation will be assessed, and the actions to be taken will be defined, ensuring the flow of information to stakeholders and the protection of critical assets.

RESPONSABILITIES

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
- Data Governance and Protection Policy
- General Data Protection Regulation (GDPR)
- Law 21.719 – Protection and Processing of Personal Data
- ISO 27001: Information Security Management
- NIST – Cybersecurity Framework

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®