GENERAL SECURITY POLICY OF THE INFORMATION

1. OBJECTIVE

The objective of the document hereof is establishing the General Policy on Information Security, pursuant to the current ISO/IEC 27001:2013 and ISO/IEC 27002:2013 standards, aiming at providing the guidelines and basic principles to safely mange the Breca Mining Division (BMD)'s information, in accordance with the business requirements and relevant regulations.

2. SCOPE

The whole staff of BMD shall mandatorily implement and comply with this policy and with the rules or regulations and procedures that derive from it.

3. RESPONSIBLE STAFF

The IT and OT Management is responsible for establishing, modifying, defining and disseminating the application of the policy hereof.

The General Manager and the Logistic and IT Management are responsible for approving and supporting the implementation of the policy hereof.

The official responsible for Information Security and the Technology Managers of our mining units are responsible of supervising compliance with the policy hereof.

The company's staff shall know and comply with the policy hereof.

4. TERMS AND DEFINITIONS

For the purposes of the document hereof, the following terms shall apply:

4.1. Information asset

4.2. Availability

4.3. Confidentiality

4.4. Integrity

4.5. Information Security

5. ESTABLISHING THE GENERAL POLICY ON INFORMATION SECURITY

5.1. Objectives

5.1.1. Align with the corporate government and create synergies with the organization's management, thus benefiting internal and external customers in terms of trust in the process information.

5.1.2. Respond to and meet the regulatory requirements related to Information Security.

5.1.3. Protect BMD's information assets against internal or external threats, whether deliberate or accidental, aiming at ensuring compliance with information confidentiality, integrity and availability.

5.1.4. Encourage the staff's participation by raising awareness on the best information security practices.

5.1.5. Prevent and reduce information security incidents by handling them on time.

5.2. Statement of the General Policy on Information Security

"In our company, information is a fundamental asset for providing our services and making decisions. Thus, we have made an explicit commitment to protect information, preserving its confidentiality, integrity and availability, through a management approach that is based on continuous improvement, risk managements and the consolidation of a culture of safety; aiming at preventing and mitigating impacts in our organization."

5.3. Specific related policies

The General Policy on Information Security is supported by a series of policies that provide principles and guidance on specific information security aspects that include:

5.3.1. Specific Policy on Information Security

It sets forth information security guidelines for BMD, in relation to its definition, approval, communication and review.

DM-POL-TI-01.02 V-003 Specific Policy on Information Security.

5.3.2. Specific policy on Information Security Organization

Guidelines for managing security within BMD (Roles, responsibilities and organizational structure). DM-POL-TI-01.03 V-003 Specific Policy on Information Security Organization.

5.3.3. Specific policy on Access control

It aims at controlling logical access to information.

DM-POL-TI-01.04 V-003 Specific Policy on Access Control.

5.3.4. Specific policy on Operation Security

To ensure the appropriate and safe operation of information processing areas.

DM-POL-TI-01-05 V-003 Specific Policy on Operation Safety.

5.3.5. Specific policy on Communication security

To ensure the protection of information in networks and its supporting information processing facilities; and the transfer of information.

DM-POL-TI-01.06 V-003 Specific Policy in Communication Security.

5.3.6. Specific policy for system procurement, development and maintenance

It aims at ensuring incorporation of security measures into information systems from their development and/or implementation and during their maintenance.

DM-POL-TI-01.07 V-003 Specific policy for system procurement, development and maintenance.

5.3.7. Specific policy on Information Security aspects in business continuity management

Aims at ensuring that business continuity is embedded into the business continuity management systems.

DM-POL-TI-01.08 V-003 Specific Policy on Information Security aspects in business continuity management.

5.3.8. Specific policy on asset management

It aims at maintaining and properly protecting all information assets.

DM-POL-TI-01.09 V-003 Specific policy on asset management.

6. ANNEXES

Annex 1 – DM-TER-TI-01.01 V-003 Information Security Terms and Definitions

Lima, June 1, 2021

Juan Luis Kruger Sayán
General Manager