INFORMATION TRANSFER POLICY.

CODE: GA010045

VALIDATION PATH		
FUNCTION	POSITION	ORGANIZATIONAL UNIT
ELABORATED BY:	Head of Technology Risk	Technology Risk
REVIEWED BY:	Members of the Security Committee	Security Committee
APPROVED BY:	Members of the Security Committee	Security Committee

Content

1 Version Control

Current version

Version	Made by	Date	Reviewed by	Date	Approved by	Date
00	Head of Technology Risk	2021	Members of the Security Committee	2021	Members of the Security Committee	2021

Version history

Version	Effective as of	Detail of changes

2 Goal

The purpose of this policy is to establish guidelines for the protection of information exchanged with external entities.

3 Scope

This Policy applies to all the companies that make up Andinas Group (Aguas Andinas S.A., Aguas Cordillera S.A., Aguas Manquehue S.A., Gestión y Servicios S.A., Análisis Ambientales S.A., Ecoriles S.A. and Aguas del Maipo S.A.), and must be observed by all persons who are part of these companies at all levels (directors and employees), acting in Chile or abroad. Also other third parties acting on behalf of the company.

Additionally, it applies to all companies, subsidiaries and associations in which any company of Andinas Group has control. In those cases in which the company lacks such control or has equal participation with other partners, it should be urged to adopt and implement policies and measures that contribute to protect the company's information.

All information to be sent to external entities and third parties in general.

Reaches collaborators in charge of information exchange processes with external entities.

Involves the information assets involved in the transfer of information outside the Group.

4 Definitions

Not applicable.

5 Roles and Responsibilities

Security Committee

- To authorize changes to the Policy.

Information Security Officer

- To ensure the implementation of this policy.
- To identify situations in which information is exchanged with third parties.
- To define the security conditions to be met in the transfer of information outside.

Collaborators

- Collaborators involved in information transfer processes outside the Group must comply with this policy.

6 Policy Description

6.1 General information

1. Andinas Group has established security measures that seek to protect the availability, confidentiality and integrity of information and privacy of personal data. One of the situations that present a risk to the information is when some information must leave the protected environment of the company and be sent to a third party, using private or public communication networks.

2. Andinas Group has defined this policy for the transfer of information with third parties, which is aimed at protecting the information that may be accessed or used by suppliers or third parties of the Group.

6.2 Relation with external entities

1. To safeguard information transfers and mitigate the dangers that may result in leakage, unauthorized access or loss of integrity, Andinas Group has defined requirements for the transfer of information between the Company and third parties, which include:

   I. Before any transfer of information outside the organization, the risk that this situation represents for the company must be evaluated and a decision must be made as to whether this action is permitted. The decision to authorize the transfer of information corresponds to the Security Committee.

   II. The Information Security Officer will define the security conditions to be established for the exchange of information.

   III. The Information Security Officer must keep an updated record of all authorized information transfer situations.

   IV. In cases of a permanent agreement for the transfer of information with a third party, this situation must be supported by a contract that formalizes the information to be transferred, the classification of this information and the protection conditions that are committed.

   Contracts should include a clause or an annex referring to information protection responsibilities.

   V. The third party must be committed to report in a timely manner any changes in the team of workers involved in the transfer of information.

   VI. Third parties with whom information is transferred will have access only to the information, equipment, information systems or facilities to which they are authorized and which are indispensable for the fulfillment of the contractual agreements.

   VII. Access to equipment, systems and information by third parties must be periodically verified and controlled by the administrators of the platforms

involved. These collaborators must inform the Information Security Officer of any situation that escapes what is agreed or permitted.

VIII. At the end of the information transfer contracts, third parties and personnel providing services must return the information or information assets that were under their responsibility and owned by Andinas Group. Likewise, the Information Security Officer will verify that the accesses assigned to the third party are eliminated due to the effects of the agreement that concludes.

6.3 Electronic communication channels

1. The Information Security Officer must determine the communication channels to be used for the exchange of information, considering the type of information to be transferred and the protections required to protect the information involved in the transfer.

2. In addition to the controls established by the Information Classification Policy, the Information Security Officer may define additional controls for the protection of data and communication channels, according to the results of the risk assessment.

7 Flow Chart

N/A

8 Appendix

N/A