INFORMATION SECURITY POLICY.

CODE: GA010032

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
00	2021	Initial version
01	11-11-2021	The Security Triad is added to the policy objectives.

2 Goal

The information generated and managed by Andinas Group is a strategic asset, key to ensuring the continuity of business services.

The purpose of this Information Security Policy is to protect information such as confidentiality, availability, integrity and non-repudiation of information. Also in its entire life cycle (creation, processing, dissemination, modification, storage, preservation and elimination), the means that allow this cycle and the people who access the information. All of the above in order to guarantee the integrity, availability, confidentiality of information and privacy of personal data.

3 Scope

This Policy applies to all the companies that make up Andinas Group or the "Company" (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.

This Policy refers to the information that the Company, its employees, customers, suppliers and third parties in general, generate, receive and/or deliver, regardless of the form in which it is presented, or in what mean it is contained, and includes the assets, tools and solutions used in the processing, storage and transmission of information.

4 Definitions

Information : Data organized and presented in a specific form. According to ISO/IEC 27000, information is an important and valuable asset for the business, therefore, it must be properly protected. It can exist in various forms: printed or written on paper, stored electronically, transmitted by mail or digital media, shown in videos or spoken in conversations.

Information Assets It refers to the information that the organization values and therefore must be protected, for which preventive measures will be taken to protect them mainly.

Responsible for the information :

Is the collaborator who receives, on behalf of the organization, the individual responsibility for the protection of a set of information. Along with the above, he/she is responsible for:

- Classify information and information assets according to defined criteria.
- Manage the labeling of assets according to the corresponding procedure.
- Authorize access, disclosure and reproduction of the information for which he/she is responsible.

Information Custodian : Is the responsible for overseeing and implementing mechanisms that guarantee the protection of the information, as defined by the Owner of the information.

Information users : Corresponds to the Company's employees and external collaborators who are allowed access to the Company's technological platforms and/or data.

5 Roles and Responsibilities

Security Committee

- To ensure the validity and currency of the Information Security Policy, specific policies and related procedures.
- To ensure the existence and proper functioning of an Information Security Management System.
- To resolve on information security priorities.
- To coordinate with other committees to maintain alignment and common management strategies.
- To report to the Directors Committee, regarding opportunities for improvement in Information Security, as well as relevant incidents and its solution.

Information Security Officer

- To organize the activities of the Security Committee.
- To develop and maintain updated security policies, control its implementation and ensure its correct application.
- To oversee the overall progress of the implementation of risk control and treatment strategies.

- To coordinate with other areas or units the support to security objectives.
- To establish points of contact with security managers of customers, suppliers and external specialists, that allow to be aware of current security trends, standards and methods.

Responsible for Information Assets

- To classify information assets according to its level of sensitivity and criticality, documenting and updating the classification carried out.
- To determine which users may have access to the information, according to their functions and competence.
- To ensure that the assets entrusted to him/her are adequately protected.

Custodians of information assets

- To execute the protection measures defined by the information owner.
- To report to the Information Security Officer, any situation that hinders or prevents the adequate protection of information assets.

Users of Information and of Information Processing Systems

- To participate in trainings and other training activities.
- To comply with the obligations imposed by the Information Security Policy and related policies and procedures.
- To report and promote the denunciation of events that conflict with the Information Security Policy, and the policies and procedures that comprise it.

6 Policy Description

6.1 Opening statements

1. The Corporate Directors' Committee is committed to promote actions aimed at achieving the information security objectives defined by the Company and to develop initiatives aimed at meeting the information security requirements, proposed by the stakeholders.

2. The Company, through the Corporate Directors' Committee, is committed to ensure the permanent improvement of the level of protection of information and the assets involved in its processing.

6.2 Guidelines

1. Information is a valuable asset and Information Systems are relevant and critical assets for Andinas Group.
2. Information Security is recognized as an indispensable attribute in the services provided by Andinas Group.
3. Information Security is defined as every action that seeks to protect the integrity, availability and confidentiality of information and the privacy of personal data.
4. Information must be protected in an adequate manner, according to its criticality.
5. The organization declares its decision to comply with the regulations and legislation in force regarding Information Security.
6. Information Security and of associated resources, is the responsibility of all internal and external collaborators of the organization.
7. All employees or collaborators of Andinas Group must have access only to the information that is strictly necessary for the performance of their duties.

8. All employees of Andinas Group have the obligation to notify any activity or situation that affects or may affect the security of information assets.
9. The organization recognizes that adequate awareness and training of its personnel in Information Security matters are priority tasks.
10. From this guideline a set of subject-specific Security Policies and its respective implementation tools are obtained.
11. The organization adheres to ISO/IEC 27001 for the implementation of an Information Security Management System, aimed at effectively and permanently reducing information risk.
12. The organization is committed to continuously improve the Information Security Management System, providing the necessary resources and training for the implementation and maintenance of this system.
13. The Security Committee provides direction on information security issues and has the authority for its Implementation and Control.
14. Changes to Andinas Group's technological infrastructure must be approved by the Information Security Officer, concerning the protection of information and information assets.
15. Failure to comply with this policy and, especially, the commission of any of the prohibited behaviors in the specific information security policies shall result in sanctions, as indicated in Policy of POL-013 Policy of Prohibitions, use of assets and disciplinary sanctions.

7 Flow Chart

N/A

8 Appendix

N/A