VALORIZA

INFORMATION SECURITY POLICY

v.1.0

INDEX

INFORMATION SECURITY POLICY

The Senior Management of VALORIZA SERVICIOS MEDIOAMBIENTALES, SA, hereinafter, "VALORIZA", within the framework of its competence to establish the general policies and strategies of the Company, has approved this Information Security Policy (hereinafter, the " Policy").

The objective of this Policy, aimed at all interest groups, is to define and establish the principles, criteria and improvement objectives that govern actions regarding information security.

1 Purpose

VALORIZA and its group of companies assume the security of the information associated with its services as one of the key factors in carrying out its activities in order to guarantee the confidentiality, integrity, availability, authenticity and traceability of the information, protecting the data and information systems against improper access and unauthorized modifications.

Part of VALORIZA's strategic policy is the implementation and development of an Information Security Management System based on the identification, protection, detection, response and recovery of information systems, with Senior Management providing the necessary resources. for its achievement.

VALORIZA understands that the processes associated with information security cannot be imposed from outside, but must be born from within the human team that makes up the Society, and encourages all its people to make information security their way of working. To this end, VALORIZA Management is committed to continually improving the Information Security Management System implemented, in the periodic reviews it maintains each year and by establishing objectives and improvement actions.

2 Area of application

This Policy applies to all subsidiary or majority-owned companies over which, directly or indirectly, VALORIZA exercises effective control regardless of their geographical location. Therefore, in all references that this Policy makes to VALORIZA, all the companies detailed above will be understood to be included.

Subsidiaries or minority-owned companies in which VALORIZA does not exercise, either directly or indirectly, effective control are not included in its scope of application, which will have, where appropriate, their own policies or regulations. internal policy that regulates the matter, and in no case may these be contrary to what is established in this Policy.

3 General principles

Through this Policy, VALORIZA and the other companies of the Group assume and promote the following general principles that must guide all their activities:

a) Direct our efforts to the prevention of errors, as well as their correction and control
b) Encourage the participation of everyone to achieve the objectives established by the company, which will benefit our clients and other interest groups.
c) Promote continuous training and awareness in information security
d) Ensure that the company meets customer requirements, in addition to applicable legal and regulatory requirements, placing special focus on those established by information security legislation.
e) Establish systematic actions for control, monitoring and prevention of security incidents
f) Equip yourself with tools and procedures that allow you to adapt quickly to changing environmental conditions.
g) Guarantee the confidentiality, integrity, availability, authenticity and traceability of information, protecting data and information systems against improper access, cyber attacks and unauthorized modifications
h) Guarantee business continuity, in terms of information security, protecting critical processes against significant failures or disasters
i) Carry out an adequate evaluation, management and treatment of information security risk to achieve a high level of maturity and minimize risk, prioritizing the measures and controls to be implemented in accordance with the identified risks and business objectives.
j) Act appropriately and jointly to prevent, detect and respond to cyber incidents that could affect information security
k) Improving the efficiency of the security controls implemented to adapt to the evolution of risks and new technological environments
l) Review and evaluate the security of the information periodically, taking the necessary measures to correct any deviations that may arise.

This information security policy has been approved by the Chief Executive Officer on November 23, 2023