INFORMATION SECURITY POLICY

The Board of Directors at Sacyr, S.A. ("**Sacyr**"), as part of their general and non-delegable duties to determine the company's policies and general strategies and following the review and proposal on the part of the Commission responsible, has approved this *Information Security Policy* (hereinafter, the "**Policy**").

The aim of this Policy, aimed at all stakeholders, is to define and establish the principles, criteria and objectives that govern activities related to information security.

1.- Purpose

Sacyr and its group of companies **("Sacyr Group")** accept information security associated to its services as one of the key factors in the performance of its activities, with the aim of ensuring availability, authenticity, integrity, confidentiality and traceability of the information, protecting data and information systems against illegal access and unauthorized modifications.

Part of Sacyr Group'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 to ensure this is achieved.

Sacyr understands that the processes associated with information security cannot be imposed from the outside, rather they should come from the company's own human team, and for this reason encourages all its staff to embrace information security in their working environment. To this end, Sacyr Group management is committed to ongoing improvement to the Information Security Management System implemented, to periodical reviews to be carried out annually, and the establishment of objectives and improvement measures.

2.- General Principles

Through this *Policy*, Sacyr and the other companies in the Group accept and promote the following general principles that shall serve as a guideline for all their activities:

a) Concentrate our efforts on error prevention, as well as correction, control and management.

b) Encourage the participation of all to achieve the objectives established by Sacyr,

which in turn will have a positive impact on our clients and other stakeholders.

c) Promote continuous training and awareness of information security.

d) Ensure that the Company complies with clients' requirements, in addition to applicable legal and statutory requirements, paying special attention to those established by legislation in the field of information security.

e) Establish systematic incident control, monitoring and preventive actions.

f) Equip itself with tools and procedures to enable it to adapt seamlessly to changing conditions in the environment.

g) Guarantee the confidentiality, availability, authenticity, integrity, confidentiality, and traceability of information, protecting data and information systems against improper access, cyber-attacks and unauthorized modifications.

h) Ensure the continuity of the business through information security, protecting critical processes against significant failures or disasters.

i) Perform an adequate assessment, 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) Improve the efficiency of the security controls implemented to adapt to the evolution of risks and new technological environments.

l) To periodically review and evaluate information security, adopting the appropriate measures to correct any deviations that may be detected.

This *Information Security Policy* was approved on September 1, 2016 and has been last amended by the Board of Directors on September 29, 2022.