CYBERSECURITY POLICY

The Board of Directors of Sacyr, S.A. ("**Sacyr**"), within the framework of its general and non-delegable competence to determine the Company's general policies and strategies, and having been reviewed and proposed by the competent Committee, has approved this *Cybersecurity Policy* (hereinafter, the "**Policy**").

The purpose of this *Policy*, which is addressed to all stakeholders, is to define and establish the principles, criteria and objectives governing actions in the field of cybersecurity.

1. Purpose

Sacyr and its group of companies ("**Sacyr Group**") consider the matter of cybersecurity associated with its services to be a key factor in how its activities are conducted, ensuring that Sacyr safeguards the confidentiality, integrity, availability, traceability, authenticity and privacy of the information and the technological assets that support it, maintaining a balance between risk levels and an efficient use of resources, following the principle of proportionality.

Likewise, these principles must be aligned with current legal and regulatory requirements and prevent impacts, for instance, on:

- Sacyr's image and reputation;
- the interruption of critical processes that underpin the business;
- the improper use of information assets;
- the loss or exfiltration of data.

The Sacyr Group's strategy includes the implementation and development of a Cybersecurity Management System that is based on national and international regulations and best practices and routed in its information systems' capabilities for identification, protection, detection, response and recovery, with Senior Management providing the necessary resources to achieve this.

Sacyr understands that this purpose must come from within the team of people that make up Sacyr, and should be part of their identity, which is why it encourages each and every one of them to incorporate it into the way they work, and share it with all stakeholders.

2. Scope of application

This *Cybersecurity Policy* is applicable to all entities belonging to the Sacyr Group, taking into account their specific characteristics. For the purposes of this document, the Sacyr Group is considered to be comprised of (i) all subsidiaries or majority-owned companies over which Sacyr, S.A. exercises effective control, whether directly or indirectly, and regardless of their geographical location, and (ii) the Sacyr Foundation. Therefore, all references in this *Policy* to the Sacyr Group are to be understood to include all of the aforementioned companies and the Foundation.

Its scope of application does not include subsidiaries or minority-owned companies in which Sacyr, S.A. does not exercise effective control, either directly or indirectly, which will instead have their own policies or internal regulations governing the matter; the latter may in no case be contrary to the provisions of this *Policy*.

3. General Principles

By means of this *Policy*, Sacyr and the other Group companies accept and promote the following general principles that must guide all of their activities:

I. Protect the information found on Sacyr's information systems.
II. Ensure that the assets belonging to the Group's companies are equipped with an appropriate level of cybersecurity and cyber resilience, making sure to apply the most advanced standards in those assets that support the operation of critical infrastructures.
III. Provide procedures and tools that allow for agile adaptation to the changing conditions of the technological environment and to new threats that arise.
IV. Raise awareness of cybersecurity risks among all employees, suppliers and other stakeholders, encouraging a culture of cybersecurity through training and awareness-raising actions. Moreover, it will be ensured that the personnel involved in cybersecurity-related duties will possess the necessary knowledge, experience and technological capabilities to meet Sacyr's cybersecurity objectives.
V. Require that appropriate cybersecurity and resilience mechanisms are in place for third-party information systems that provide services to the Group.
VI. Consider efficiency and sustainability criteria when implementing applicable cybersecurity measures.

VII. Enhance the capabilities for prevention, detection, reaction, analysis, recovery, response, investigation and coordination in the face of cyberterrorism and cybercrime threats to prevent them from impacting Sacyr, and if they do, to minimize their effects on the business.

VIII. Collaborate with relevant government bodies and agencies to contribute to the improvement of cybersecurity at a national and international level.

IX. Act in accordance with current legislation, the Code of Ethics and the Company's other internal regulations.

X. Uphold and promote the principles of this *Policy*, which will begin with the organization's Senior Management.

This *Cybersecurity Policy* was approved by the Board of Directors on December 18, 2023.