CYBERSECURITY POLICY

1. PURPOSE

ACCIONA considers information to be one of its most important assets, including the systems that support and process information. It has therefore established the objective of effective and efficient management of the risks to which information and information systems are subject.

This policy consequently establishes the cybersecurity principles in force at ACCIONA to ensure the protection of its information and the supporting systems thereof.

The specific objectives of this document are:

- Define the principles that govern the management of cybersecurity at ACCIONA and according to which the group's information is protected and the cybersecurity risks to which it is exposed are mitigated. These principles will be in line with legislative and regulatory requirements in force.
- Define and assign the responsibilities associated with the implementation and maintenance of the cybersecurity management model.
- Establish a framework that facilitates decision-making related to the implementation of cybersecurity measures, both technical measures and procedural and organizational ones, in order to prevent the following impacts:
    - Harm to the image and reputation of ACCIONA.
    - Interruption of the critical processes that support the business.
    - The loss or improper use of information assets.

2. SCOPE

This policy applies to all information assets, companies and employees of the Group, as well as to collaborators and external companies that access ACCIONA's information systems.

ACCIONA also has the obligation to ensure, under the same terms, the security of information that concerns its customers, collaborating entities and competent official bodies.

3. DEVELOPMENT OF THE POLICY

The policy is complemented by a Regulatory Framework for the management of Cybersecurity, which is appropriate for responding to current and emerging threats, as well as regulatory requirements. The structure of this regulatory framework is divided into three levels:Primer nivel normativo: constituido por la presente política.

- **First regulatory level**: formed by this policy.
- **Second regulatory level**: formed by general cybersecurity standards.
- **Third regulatory level:** formed by procedures, operating manuals and technical guides.

The Cybersecurity Regulatory Framework is reviewed regularly at least once a year, as well as after significant changes that might affect ACCIONA's cybersecurity environment and/or the circumstances of its business.

4. PRINCIPLES

- **Prevention and resilience:** strengthen capabilities for protection against and the early detection of cyber threats to prevent them from having an impact on ACCIONA, and if they do have an impact, so that their effects on the business can be minimised.
- **Participation by Senior Management:** cybersecurity is assumed as a duty whose responsibility is exercised beginning at the organization's highest hierarchical level, wherefore the Management Committee assumes the commitment to ensure implementation of the cybersecurity management system that allows putting what is defined in this document into practice.
- **Shared responsibility**: cybersecurity is a duty that requires the full cooperation of all personnel at ACCIONA, regarding not only compliance with the established standards and procedures that expressly concern them, but also any collaboration that might be occasionally required by the functional managers of cybersecurity.
- **Training:** an adequate level of training and awareness is deemed to be one of the indispensable cornerstones for the correct management of cybersecurity. ACCIONA therefore promotes a culture of cybersecurity through training actions targeted at all employees and stakeholders who are involved. Likewise, it guarantees that cybersecurity teams have the knowledge, experience and technological capability for complying with ACCIONA's cybersecurity objectives.
- **Regulatory compliance**: compliance with applicable laws and regulations related to cybersecurity in all countries where ACCIONA operates must be ensured. Likewise, ACCIONA collaborates with all competent authorities and agencies in order to contribute to the improvement of cybersecurity.

5. ORGANIZATION OF CYBERSECURITY

The Cybersecurity Management Committee is ultimately responsible for cybersecurity at ACCIONA, and it delegates the execution of this function to the Cybersecurity Director. This person reports hierarchically to the Director of Information Systems and the Director of Corporate Security. This ensures that the technical controls for which Technology and Processes Directorate is responsible are consistent and converge with the physical and personnel controls for which the Corporate Security Area is responsible.

The mission of Cybersecurity Directorate is to effectively and efficiently manage the Group's information assets, thereby seeking to ensure the viability of the business and taking charge of furthering the organization of cybersecurity defined in this policy.

The Cybersecurity Management Committee is responsible for promoting and supporting the establishment of technical, organizational and control measures that guarantee the integrity, availability and confidentiality of information, within a general framework to manage cybersecurity risks. This makes therefore such measures compatible with the necessary transmission of information and knowledge among the various organizational areas of ACCIONA.

For coordination purposes, there are different operational Cybersecurity Committees, in which the main cybersecurity managers of the different areas, functions, companies or territories that may be determined in each case participate.

Without prejudice to the preceding, every ACCIONA employee is responsible for complying with cybersecurity requirements when performing their duties, such that there is shared co-responsibility among employees, executives, collaborators and the cybersecurity organization.

6. AUDITING

Audits are periodically conducted, whether total or partial, with the objective of verifying the level of compliance with what is defined in ACCIONA's Cybersecurity Regulatory Framework.

7. VALIDITY AND REVISIONS

This policy will enter into force on the next business day following the approval hereof by the ACCIONA Cybersecurity Management Committee. It will remain in force as long as it is not amended or revoked by a subsequent policy.

Any exceptions to the provisions set forth in this policy will be dealt with and approved by the ACCIONA Cybersecurity Management Committee.

As from the entry into force hereof, a period of three months is provided for adapting the incompatibilities of the provisions set forth in this document to those that could exist in other standards, both global and local.

This document will be revised not only periodically but also according to the organizational, legal or business changes that could occur at any given time in order to maintain its pertinence, sufficiency and efficacy. If changes are made to the document, they will be communicated and published in the Cybersecurity space of ACCIONA's Intranet (InterACCIONA).

This policy is available on the Intranet (InterACCIONA) to all employees and on the corporate website to all stakeholders of the company.

This policy will come into force on the next business day following its approval by the Audit and Sustainability Committee of the Board of Directors of ACCIONA, SA. It shall remain in force until it is modified or repealed by a subsequent policy.

Exceptions to the provisions of this policy will be dealt with and approved by the Audit and Sustainability Committee of the Board of Directors of ACCIONA, SA at the proposal of ACCIONA's Cybersecurity Management Committee.

December 16, 2022

.