CYBERSECURITY POLICY

PREPARED BY	REVIEWED BY	APPROVED BY
Juan Carlos Sánchez Soto Cybersecurity and IT Risk Manager, ACCIONA Energía **SIGNATURE** Date: 31/05/2023	**Carlos Pérez Castelló** ACCIONA Energía Safety Director **SIGNATURE** Date: 01/06/2023	**ACCIONA Energía Cybersecurity Steering Committee** **SIGNATURE** Date: 01/06/2023

Version Control

Version	Date	Description
1.0	01/06/2023	Original version

TABLE OF CONTENTS

1. INTRODUCTION

ACCIONA Energía considers information, together with the systems used to contain and process it, one of its most important assets, which is why we aim to effectively and efficiently manage information-related risks.

2. PURPOSE

This document discusses the cybersecurity principles ACCIONA Energía has adopted to protect our information and the systems that support it.

The specific objectives of this document are:

- To define the governing principles of cybersecurity management at ACCIONA Energía aimed at protecting the group's information, mitigating the cybersecurity risks to which that information is exposed and complying with current regulatory requirements.
- To define and assign the responsibilities associated with the implementation and maintenance of the cybersecurity management model.
- To establish a framework that facilitates decision-making with regard to the implementation of technical, procedural and organisational cybersecurity measures in order to prevent the following impacts:
    - Damage to the image and reputation of ACCIONA Energía.
    - Interruption of critical business processes.
    - Loss or misuse of information assets.

3. SCOPE

This policy applies to all information assets and employees of ACCIONA Energía, subsidiaries and affiliates of ACCIONA Energía, as well as collaborators and external partners who have access to the information systems of ACCIONA Energía.

ACCIONA Energía has an obligation to guarantee the security of the information pertaining to its customers, partners and official organisations in the same terms.

4. DEVELOPMENT OF THE POLICY.

This document is derived from the Cybersecurity Policy of ACCIONA, S.A., so that the regulatory and procedural development of this document aligns with the existing Cybersecurity Policy of ACCIONA, S.A. but also addresses the specifics of ACCIONA Energía's particular cybersecurity policy. It is reviewed regularly, at least once a year, and any time there are significant changes that affect the cybersecurity environment in which ACCIONA Energía operates and/or its business circumstances.

5. PRINCIPLES

The principles governing cybersecurity management at ACCIONA Energía are as follows:

- **Prevention and resilience**: It is essential to reinforce the capability to protect against cyberthreats, to detect them early, prevent them from materialising and minimise their effects on the business.
- **Involvement of Senior Management**: Cybersecurity is a responsibility that is assumed at the highest hierarchical level of the organisation. In keeping with that commitment, the Cybersecurity Steering Committee has made a commitment to ensure the implementation of the cybersecurity management system and in so doing put into practice the contents of this document.
- **Shared responsibility**: Cybersecurity is something that requires the active collaboration of all ACCIONA Energía personnel. This includes compliance with the established rules and procedures that expressly apply to them and collaboration that may be required from time to time by those responsible for cybersecurity.
- **Training**: One of the basic pillars of effective cybersecurity management is proper training and awareness. ACCIONA Energía promotes a culture of cybersecurity through training actions for all employees and stakeholders. We also ensure that the cybersecurity teams have the knowledge, experience and technological capabilities to achieve the cybersecurity objectives of ACCIONA Energía.
- **Regulatory compliance**: It is crucial to ensure compliance with the cybersecurity laws and regulations in all countries where ACCIONA Energía does business. ACCIONA Energía also collaborates with the competent authorities and other organisations to enhance cybersecurity.

6. CYBERSECURITY ORGANISATION

The Cybersecurity Steering Committee is the body ultimately responsible for cybersecurity at ACCIONA Energy, having delegated the performance of this function to the Cybersecurity Manager. The person in this role reports hierarchically to ACCIONA Energía's Technology Department and ACCIONA Energía's Security Director. This ensures the coordination and consistency of the technical controls which are the responsibility of the Technology Department and the physical and personal controls which are the responsibility of the Corporate Security area.

The mission of Cybersecurity Management is to effectively and efficiently protect the company's information assets, ensuring the viability of the business and promoting the cybersecurity principles defined in this policy.

The Technology Department at ACCIONA Energía is responsible for promoting and supporting the establishment of technical, organisational and control measures that guarantee the integrity, availability and confidentiality of information within a general framework of cybersecurity risk

management, whilst at once enabling the necessary transmission of information and knowledge between the different areas of the ACCIONA Energía organisation.

For coordination purposes, there are different Cybersecurity Committees whose members include cybersecurity managers from different areas, enterprises or territories, as determined on a case-by-case basis.

However, all ACCIONA Energía employees are responsible for abiding by cybersecurity requirements in the performance of their duties. In other words, there is a shared responsibility between employees, managers, partners and the cybersecurity organisation.

7. AUDIT.

Partial or full audits are carried out periodically in order to verify the level of compliance with the principles laid out in the Cybersecurity Regulatory Corpus.

8. VALIDITY AND REVISIONS

The policy comes into force on the next business day after its approval by the ACCIONA Energía Cybersecurity Steering Committee. It remains in force until it is modified or repealed by a later policy.

Exceptions to the provisions of this policy are dealt with and approved by ACCIONA Energía's Cybersecurity Steering Committee.

From the time it takes effect, ACCIONA Energía has three months to correct any incompatibilities that may exist between the provisions of this document and those of other local or global regulations.

This document is reviewed periodically in light of organisational, legal or business changes that may be introduced from time to time in order to maintain its relevancy and effectiveness. Any changes that are made are notified and published in the Cybersecurity section of the ACCIONA Energía Intranet (InterAcciona) and in the MAP system.

This policy is available to ACCIONA Energía staff on the Intranet (InterAcciona), to the company's stakeholders on the corporate website and in the MAP system.