ALMIRALL, S.A.	BOARD OF DIRECTORS

INFORMATION SECURITY POLICY

1- Introduction

The purpose of this Policy is to establish basic principles relating to the prevention of risks in the use of Company information or that related to it, according to the following objectives: (i) define Almirall's principles and governance structure to ensure the protection of Information Security's key dimensions (confidentiality, availability and integrity), (ii) define the internal regulatory system for control and management of Information Security, and (iii) define guidelines for risk management on Information Security.

2- Principles

The Almirall Information Security Policy is based on the following principles:

-Information Security strategy should be aligned with business objectives and strategy.

-Information Security must have a dedicated organizational structure and explicit endorsement by the Management Board as a critical function.

-Governance mechanisms must ensure Information Security's independence with regards to risk identification, assessment, monitoring and reporting.

-Information is a strategic asset for Almirall, so it is essential to protect it from risks that may affect confidentiality, integrity, availability and traceability.

-Security measures and controls should be implemented following a risk-oriented approach. This applies to the entire life cycle of the information and IT assets.

-Information assets should be classified, also ensuring that they are only accessible to authorised users, according to the level assigned.

-The information processed and exchanged with natural or legal persons, regardless of its owner, must comply with the requirements in relation to Almirall's Information Security, as well as current legislation applicable, including Privacy regulations such as GDPR.

-All employees with access to Almirall information should be trained on a regular basis, and made aware of existing risks.

Barcelona, May 6, 2021