INFORMATION SECURITY & QUALITY

Guidelines & Principles

Contents

1. INTRODUCTION

The working philosophy of Board International SA (hereinafter also referred to as "**Board**" or the "**Company**" or the “**Organization**”) is based on a commitment to quality, information security and privacy, in order to achieve the satisfaction of stakeholders (such as customers and partners) and to meet their requirements, expectations and needs to the fullest extent possible.

For this reason, the Company has decided to implement an Integrated Management System (IMS) for Board SaaS service and related processes and activities based on the following standards:

- UNI EN ISO 9001:2015 *Quality management systems*
- ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*
- ISO/IEC 27017:2015 *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- ISO/IEC 27018:2019 *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*

This document contains the guidelines and general principles of Board's corporate mission and its objectives in terms of:

- creating value for all stakeholders, guaranteeing product and service quality to meet customer expectations and consolidate the image achieved in its sector, and complying with compliance obligations.
- protection and preservation of information assets as a strategic and indispensable value factor that can turn into a competitive advantage in the provision of services.

This document has been approved by a resolution of the Board of Directors on November 13, 2024. Any amendments or updates are subject to the approval of the Company’s Board of Directors.

2. GENERAL PRINCIPLES

This integrated quality and information security management system aims to regulate the organisational and technical activities of Board in a systematic, planned, documented manner, aimed at satisfying the specified requirements, managing business risks and continuous improvement, while respecting the context in which the company operates and the expectations of its interested parties.

Furthermore, through the implementation of its Integrated Management System, Board aims to:

- create a culture of quality and information security among its employees, making them aware of the importance of each individual's role;
- plan its IMS based on the Risk Based Thinking approach and govern the identified risks;
- adequately manage any deviations and incidents in terms of prevention, timely recognition and treatment;
- meeting customer requirements;
- continuously adapt the company's production capacity and flexibility in order to maintain a high level of product and service competitiveness;

- be aware of the information managed within the scope of its activities and assess its criticality in order to implement adequate levels of protection;
- be compliant with applicable laws and regulations, respect the security commitments set out in contracts with stakeholders and comply with company procedures; and
- constantly monitor process trends and, based on these, set and achieve performance improvement targets.

Board is committed to playing an active role in the promotion of all activities that have an influence on the Integrated Management System through:

- the dissemination and knowledge, at all levels and for all interested parties, of the concepts expressed in the procedures and policies forming an integral part of the Integrated Management System;
- the full availability of the means and resources necessary for the implementation and maintenance of this Integrated Management System;
- the dissemination of instructions for the correct handling of information and personal data and any information security incidents, anomalies or possible threats;
- operational support for the effective adoption and implementation of the IMS, periodic review and continuous improvement.

2.1 Quality

With regard to Quality, Board is committed to carrying out its activities and delivering the Board SaaS Service according to UNI EN ISO 9001:2015, respecting the following principles:

- seeking the satisfaction of the needs and expectations of all stakeholders relevant to the achievement of the organisation's objectives.
- to create a partnership relationship with customers by working proactively to offer them more opportunities to use our solutions to support their business.
- ensuring the correct sizing of the organisational structure with an appropriate distribution of competencies.
- ensuring continuous trainings and increase the competence of our personnel.
- to guarantee this competence, processes have been defined for managing training and monitoring its effectiveness.
- improve existing processes and manage innovation in order not only to respond to evolving needs, but to anticipate potential changes in the context, to maintain competitive advantage and seize new opportunities.
- define policies and methods to monitor, evaluate, optimise and protect resources in a manner consistent with the strategy.
- ensure the quality of the product supplied.
- monitoring our suppliers through certain indicators on aspects relevant to Board.

The measurement of our customers' satisfaction is the benchmark for the implementation of improvement programmes. It is based on:

- the direct detection of customer satisfaction through interviews
- the detection of Complaints spontaneously communicated by customers to Board; and
- on the formal detection of Customer satisfaction through questionnaires administered to our customers.

2.2 Information Security

Regarding the Information Security and Privacy, the Company undertakes to carry out its activities according to the standard of ISO/IEC 27001:2022 with extensions ISO/IEC 27017:2015; ISO/IEC 27018:2019 respecting the following principles:

- against the identified and assessed risks, define a set of organizational, technical and procedural measures to ensure that security is maintained and the basic security requirements listed below are met:

  - *Confidentiality*, i.e. the property of the information to be known only to those with privileges;
  - *Integrity*, i.e. the property of the information to be modified only and exclusively by those who have the privileges;
  - *Availability*, i.e. the property of the information to be accessible and usable when requested by the processes and users who have the privileges;

- know and assess the criticality of the information managed, including personal data, for the implementation of adequate levels of protection.
- set up organizational, procedural and technological security measures to protect information security and privacy, including in the cloud through the implementation and maintenance of business continuity plans.
- promote a culture of information security (including personal data) and develop awareness programmes to provide adequate training on how to manage it.
- ensuring the adoption and maintenance of a process for identifying potential threats to the company and the impacts that such threats, if realized, could cause on the information assets and services provided.
- manage any security incidents (including possible breaches of personal data) and continuity and take appropriate countermeasures.
- ensuring compliance with legal requirements, reference standards and security commitments set out in contracts with stakeholders.
- promote collaboration with qualified technology partners that guarantee reliability in terms of the quality of the services offered and the security of information.

2.3 Continuous Improvements

The Company aims to pursue, also with a view to continuous improvement:

- the effectiveness and efficiency of its processes and of the Integrated Management System in general;
- the effective management of any non-conformities, incidents and anomalies encountered and the prevention of potential non-conformities through all the activities performed.
- increasingly reducing all causes of inefficiency.

The pursuit of the improvement objectives relating to the principles listed above is implemented through the application of the policy and procedures defined as part of Integrated Management System.

This document is periodically reassessed in order to adapt it to any regulatory, technological, organisational, economic and social changes.