General Information Security Policy

Take The Wind, S.A.

IDENTIFICATION

- Available and communicated to the entire organization.
- Public use.
- Ownership of Take The Wind and may not be used for other purposes than those for which it has been distributed, or reproduced, in whole or in part, or transmitted or communicated to any person without authorization from the Management.

INDEX

INTRODUCTION

This Information Security Policy serves as the basis for the information security management system, respecting the international standard ISO / IEC 27001: 2013, community standards and specific national legislation and recommendations in the area of information security.

Take The Wind, when establishing the Information Security Management System (ISMS), assumes the present policy, integrating the ISMS requirements in the organization's processes and ensuring that the necessary resources for its implementation are available. It has the responsibility of acting appropriately with regard to information security management, as well as to monitor and evaluate the ISMS implementation.

This document describes the general principles that must be applied by each of Take The Wind's business units and the information assets managed by it, being structured as follows:

- Audience;
- Information Value;
- Importance of Information Security;
- Information Security Model;
- Information Security Objectives at Take The Wind;
- Responsibility in Information Security;
- Maintenance and Communication of Security Policies;
- Continuous improvement of the ISMS.

AUDIENCE

Take The Wind's Information Security Policy is aimed at all interested parties/stakeholders.

All interested parties must know and act in accordance with the Take The Wind's Information Security Policy and with other documents related to Information Security, as applicable and appropriate.

All interested parties who are covered by the ISMS and who deliberately violate this or other policies will be subject to sanctions and other actions, which may include termination of the contract and / or reporting to the police or judicial authorities in situations that indicate the practice of crime.

INFORMATION VALUE

Information can take different forms (be it printed or written on paper, stored electronically, transmitted by email or electronic means, among others), and must be adequately protected, regardless of its medium, use or support. Information security should be adjusted to its importance and value.

Access to information is an important aspect of Take The Wind's functioning, depending on the availability of infrastructures and information systems and the efficiency of the service provided to its customers. Security in the treatment and transmission of information is therefore a vital factor in maintaining its efficiency.

Any interruption of service, leakage of information to unauthorized entities or unauthorized modification of data, can lead to a loss of confidence and / or violate obligations to interested parties.

In order to achieve the objectives regarding information security, Take The Wind's business units depend on the correct and expected functioning of their information systems. However, this is only possible with the continuous identification of the risks to which Take The Wind assets are exposed, as well as, by the implementation of controls and security mechanisms aimed at their correct and controlled use.

Information security is a fundamental prerequisite for the success of the services provided by Take The Wind and it is the responsibility of all employees, suppliers or other entities, to proactively contribute to the protection of sensitive information by any means, including verbally.

IMPORTANCE OF INFORMATION SECURITY

The information managed by Take The Wind, its support processes, systems, applications and networks are valuable assets for Take The Wind.

The loss of confidentiality, integrity and availability can lead to a loss of credibility for the services provided by Take The Wind.

Information security should be applied at all stages of the ISMS. The control of the insertion, collection, processing, storage, transfer, relationship, research and destruction of information operations are an integral part of Take The Wind's information system.

The maintenance, in a permanent and balanced way, of a high level of quality and security, prevents the materialization of inherent risks and limits the potential damages caused by the exploitation of vulnerabilities and security incidents, ensuring that the business operates as expected over time.

Threats to information security are constantly evolving, which implies the continuous adaptation of security measures in order to keep up with technological, legislative and / or social changes. Security measures must be technically and economically viable, and must not inappropriately limit Take The Wind's productivity and efficiency.

The residual risk must be approved by the Management and by those responsible for the unit who have operational responsibilities over the associated assets.

The Information Security Policy, described in this document, has the main objective of establishing Take The Wind's global information security guidelines.

In this sense, this Policy establishes the guidelines for the effective management of information security in the following areas:

- Human resources management: Information Security is applicable to all of Take The Wind's employees, with specific responsibilities for each role;
- Risk management: All systems (existing or planned) must have an adequate level of security in view of the risk that Take The Wind is willing to take. A risk analysis must reflect technical concerns so that they are easily interpreted by the business;

- Definition of responsibilities: Responsibility for the quality, access, use and safeguarding of the information contained in the systems rests with those responsible for that data. Take The Wind is responsible for defining the rules and procedures that implement the levels of information security defined by the entities that own the information and monitor its effectiveness.
- Security policies: There must be security policies that define the objectives to be achieved by all information systems, regardless of their environment;
- Security procedures: Development of detailed procedures that define “what” and “how” to achieve the desired level of security;
- Proper future operation of information systems: Information system operations must be properly documented, ensuring that at any time it is possible to assess “who” and “when” does “what”;
- Do what is right: Information security is a responsibility of Take The Wind.
- Know what is happening: The implementation of controls that address the risks to which the business is exposed, is only effective if there is adequate monitoring of the controls, in order to assess whether they are adjusted to the defined objectives. Equally, actions for timely response should be defined when controls are not operational.

INFORMATION SECURITY MODEL

Take The Wind’s information security model is committed to:

- Confidentiality: guarantee that the information is accessible only by people authorized for the purpose;
- Integrity: safeguarding the accuracy of information and processing methods;
- Availability: guarantee that authorized users have access to information whenever necessary.

All existing security mechanisms at Take The Wind address confidentiality, integrity and availability of information. They must be regulated by a normative body made up of security policies and procedures, structured according to the InformationSecurity Management System Manual.

The document "General Information Security Policy" has the main objective of defining the value of Information Security for Take The Wind and describe its importance.

INFORMATION SECURITY OBJECTIVES AT TAKE THE WIND

Take the Wind presents its policy with appropriate measures that ensure the implementation of the ISMS based on the international standard ISO 27001.

RESPONSIBILITY IN INFORMATION SECURITY

Take The Wind's business units, together with IT must implement the Information Security Policy.

The Policies for Information Security define the control objectives, as they should be applied to Take The Wind.

Top management is committed to meet the applicable information security requirements and continuously improving the Information Security Management System.

The Chief Information Security Officer (CISO) and its backup lead the management and coordination structure for the implementation of the Information Security Management System.

MAINTENANCE AND COMMUNICATION OF SECURITY POLICIES

Information security policies and standards must be reviewed annually ensuring that they remain relevant and appropriate for Take The Wind and must be known by all employees within each scope of application. In this sense, the procedures necessary for its review and disclosure should be defined, as follows:

- Ensure that policies are observed and reviewed, if necessary, to remain in line with Take The Wind's reality;
- Ensure the availability of all documentation to all employees within its scope.

- Ensuring effective communication of the information security policies and standards to all employees so that they are aware of individual obligations regarding the topic of information security.

CONTINUOUS IMPROVEMENT OF THE INFORMATION SECURITY SYSTEM

A high level of quality and security must be ensured in a permanent and balanced manner, preventing the materialization of inherent risks to mitigate / limit the potential damage caused by the exploitation of vulnerabilities and information security incidents. The threats to information security are constantly evolving, which implies the continuous adaptation of information security measures in order to keep up with technological and legislative or regulatory changes. Information security measures must be technically and economically viable and must not limit Take The Wind's productivity and efficiency.

Version History						
Version	Editor	Approver	Approval Date	Update Description	Revision Date	Reviewed By
1.0	Ricardo Seco	Pedro Pinto	17-11-2023	First version of the document	21-02-2024	Marisa Campos