Policy

Information Security Policy

NWP

CORP-NWP-25-0013-R00

nabla wind hub

DOCUMENT DESCRIPTION

CLIENT: NWP

PROJECT: Information Security Policy

CODE: CORP-NWP-25-0013-R00

RECORD OF CHANGES:

2025-10-17: R00 | Registro inicial

PREPARED	CHECKED	APPROVED
Pablo Villasante	*Eder Murga*	*Alfonso San Emeterio*
IT Manager	Head of Operations	General Manager

TABLE OF CONTENTS

1. OBJECTIVE AND SCOPE OF APPLICATION

Nabla Wind Power SLU., an independent engineering company dedicated to the redevelopment of wind farms through techniques that combine Life Extension, Performance Improvement, and Operation and Maintenance Optimization (based on site conditions), has decided to implement an Information Security Management System based on the ISO 27001 standard. The objective is to preserve the confidentiality, integrity, and availability of information and protect it from a wide range of threats. This Management System is designed to ensure business continuity, minimize losses, maximize return on investment and business opportunities, and continuously improve information security.

2. DEVELOPMENT

Management recognizes that information is a highly valuable asset for the Organization and its stakeholders; therefore, it requires adequate protection. Furthermore, it establishes the following as fundamental objectives, starting points, and support for the specific objectives, principles, processes, and actions of information security:

- Protect personal data and the privacy of individuals.
- Safeguard the organization's information assets from the security dimensions of confidentiality, availability, and integrity.
- Protect intellectual property rights.
- Comply with and enforce this Information Security Policy.
- Assign roles, functions, and responsibilities to preserve information security.
- Record and properly address security incidents.
- Manage business continuity.
- Provide training, capacity building, and awareness programs for information security.
- Manage any security-related changes that may occur within the company. Similarly, the Management of Nabla Wind Power SLU, through the development and implementation of this Information Security Management System, undertakes the following commitments:
- Development of products and services that comply with legal requirements, identifying the applicable legislation for the business lines developed by the organization and included within the scope of the Information Security Management System.
- Risk management focused on continuous improvement and the protection of the organization's information assets.
- Establishment and compliance with contractual requirements with stakeholders.
- Definition of security training requirements and the necessary training in this area for stakeholders through the establishment of training plans.
- Prevention, detection, and response to viruses and/or any other malicious software, as well as incidents and cyber incidents related to information security, through the development and application of specific policies and processes and the establishment of contractual agreements with specialized organizations.
- Business continuity management, developing continuity plans in accordance with internationally recognized methodologies.
- Establishing the consequences of security policy violations and reflecting them in contracts signed with stakeholders, suppliers, and subcontractors.
- Raising awareness and assessing the impact of climate change within the organization.

Conducting all activities in accordance with the strictest professional ethics. This Policy provides the framework for the continuous improvement of the Information Security Management System, as well as for establishing and reviewing its objectives. Its scope encompasses "the management of information security that supports the technical engineering services for the redevelopment of assets in the wind energy sector, according to the current Statement of Applicability" [*]. This Policy is widely disseminated throughout the Organization via the document management

system installed within the organization and published in informational environments. It is reviewed annually for its continued suitability and on an extraordinary basis when special situations and/or substantial changes occur in the Information Security Management System. It is also available to the general public.

[*] Not applicable: 8.11 Data Masking / 8.30 Outsourced Development

nabla
wind hub