Policy

Privacy and Digital Security Policy

NWP

CORP-NWP-23-0005-R01

nabla wind hub

DOCUMENT DESCRIPTION

CLIENT: NWP

PROJECT: Privacy and Digital Security Policy

CODE: CORP-NWP-23-0005-R01

RECORD OF CHANGES:

2023-09-19: R00 | Initial Issue

2024-02-21: R01 | First change: Add the KeePassXC digital tool

PREPARED	CHECKED	APPROVED
Paola Salcedo	*Ahmed Moussa*	*Alfonso San Emeterio*
Marketing&Comms Manager	Head of BD	General Manager
Naiara Puentes	*Eder Murga*	
Bids and Proposals Manager	Head of OPS	
	Pablo Villasante	
	IT Manager	

Relevant information of the document and disclaimer

This document is for the use of the Customer, as per detailed on the first page of this document, and has been made in agreement with and according to the Customer's instructions. To the extent permitted by law, Nabla Wind Hub does not assume any responsibility whether in contract, tort including without limitation negligence, or otherwise howsoever, to third parties (being people other than the Customer).

This document has been prepared by Nabla Wind Hub with information provided by the Customer and/or third parties. This document has been produced based on information relating to dates and periods referred to in this document. Nabla Wind Hub is not responsible for the validity of such information, and the document does not imply that any information is not subject to change. Except and to the extent that checking, or verification of information or data is expressly agreed within the written scope off its services, Nabla Wind Hub shall not be responsible in any way in connection with erroneous information or data provided to it by the Customer and/or any third party, or for the effects of any such erroneous information or data whether or not contained or referred to in this document.

Any of the outputs reflected in this document are subject to factors, not all of which are within the scope of the probability and uncertainties contained or referred to in this document and nothing in this document guarantees any wind speed or energy output.

This document must be read in its entirety and is subject to any assumptions and qualifications expressed therein as well as in any other relevant communications in connection with it. This document may contain detailed technical information which is intended for the use only by people possessing the required expertise in the matter.

TABLE OF CONTENTS

1. PRIVACY AND DIGITAL SECURITY POLICY

Nabla Wind Power S.L.U. aims to create a secure environment for all its employees, as well as for third parties involved in our day-to-day operations, such as customers and suppliers.

The more we rely on technology for our daily work, the more vulnerable we become to serious security breaches (such as human error, cyber-attacks or system malfunctions). For this reason, Nabla Wind Power S.L.U. has developed this policy with the aim of establishing comprehensive guidelines for the security and privacy of information and services.

This policy applies to all employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

2. CONFIDENTIAL INFORMATION

All confidential data is sensitive and valuable, such as:

- Financial information,
- Data relating to customers, partners or suppliers,
- Patents, formulas or new technologies,
- Customer lists.

All employees are required to protect this data. In this policy, we will provide our employees with guidance on how to prevent security breaches.

3. PROTECT PERSONAL AND COMPANY DEVICES

When employees use their digital devices (e.g. computers or phones) to access company emails or accounts, they pose a security risk to our data.

The best advice for employees is to use these devices solely for work-related purposes and not for personal use. Furthermore, it is advisable to:

- Keep all devices password-protected,
- Use comprehensive antivirus software (e.g. Microsoft 365 Defender for Azure, as well as Kaspersky),
- Ensure that devices are protected at all times and are not left exposed or unattended in public spaces,
- Log in to company accounts and systems only via secure, private networks (e.g. VPN),
- Install browser and system security updates monthly or as soon as updates are available,
- Avoid accessing internal systems and accounts from third-party or personal devices.

Should new recruits receive any type of digital device, they will receive instructions from our IT Manager, Pablo Villasante. If they have any further questions or concerns, they should contact the aforementioned manager.

In addition, we have a new cloud-based tool to help us manage our devices and applications called Intune, from which we can install applications and adjust security settings all in one place. It's like having a remote control, ensuring that all our devices are protected and up to date.

4. SECURE EMAILS

Emails often contain scams and malicious software (such as worms or viruses). To prevent virus infections or data theft, it is important that employees:

- Avoid opening attachments and clicking on links whose content is not explained (e.g. clicking on suspicious images),
- Do not fall for clickbait headlines (e.g. discounts, free tips),
- Check whether the email address and the names of the senders are legitimate,
- Look out for strange or suspicious errors (e.g. grammatical errors, nonsensical words).

If you receive a suspicious email, please contact our IT manager, Pablo Villasante, as soon as possible.

5. MANAGE PASSWORDS PROPERLY

Password leaks are dangerous as they compromise the entire digital infrastructure of Nabla Wind Power S.L.U. All passwords must be secure and kept secret so that they cannot be easily hacked. For this reason, employees should:

- Choose passwords of at least eight characters (including upper- and lower-case letters, numbers and special characters). Avoid using personal information (e.g. birthdays, names) and use different passwords; do not use the same one for everything,
- Memorise passwords and do not write them down,
- Only share this information if absolutely necessary,
- It is recommended that you change your password every two months for security reasons.

If you need to have a set of shared passwords for several people, use a specialised programme to store this type of information with maximum security; it is called KeePassXC.

6. TRANSFERRING DATA SECURELY

When transferring data between colleagues, it is very important to follow these guidelines:

- Avoid transferring sensitive data (e.g. customer data, employee data) to other devices or accounts outside the workplace. In the event of a large-scale transfer of this type of data, the employee should contact the IT manager for assistance.
- Share data via the company network/system and not via public Wi-Fi or private connections.
- Ensure that the recipients of the data are authorised to receive it.
- Always report potential scams, privacy breaches and hacking attempts.

It is very important that our IT Department is aware of scams, breaches and malware so that it can protect our infrastructure. For this reason, we advise our employees to always report any concerns in this regard. Our IT Department is responsible for advising employees on how to spot fraudulent emails.

7. REMOTE WORKERS

Employees working remotely must also comply with the instructions set out in this policy. As they access our company's accounts and systems remotely, they are required to adhere to all encryption and data protection standards and settings, and to ensure the security of their private network.

8. ADDITIONAL MEASURES

Here are some further recommendations to follow:

- Turn off screens, lock devices when leaving, and avoid keeping passwords written down in the workplace,
- Report stolen or damaged equipment to the IT Department as soon as possible,
- Change the password for all accounts if a device is stolen,
- Do not download suspicious or unauthorised files onto company equipment,
- Avoid accessing suspicious websites.

Everyone, from our customers and partners to our employees and contractors, must feel that their data is secure. The only way to earn their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cybersecurity firmly in mind.

This policy has been approved by the Managing Director of Nabla Wind Power S.L.U., Alfonso San Emeterio, the IT Director, Pablo Villasante, and the Head of Operations, Eder Murga, on 19 September 2023. It will be reviewed periodically on an annual basis to incorporate any necessary modifications and updates, with the aim of improving its effectiveness.

This policy will be made available to all employees via the standard channels in all departments, as well as on the corporate website.

nabla
wind hub