Windar renovables

Information security basic rules

GD000737-R.01

Index

1. Objective
2. Use of information
3. Use of Information systems and & resources
4. Prohibited, illegal or unacceptable uses
5. Supervision and verification of acceptable use
6. Information exchange
7. Access Control Policy
8. Email use policy External
9. Media use policy
10. Responsible use of the Internet. Navigation restrictions.
11. Use of software licenses
12. Processing of personal data
13. Incident management
14. Use of corporate mobile phones
15. Information Security Organization
16. Control and monitoring programs and devices
17. Use of artificial intelligence
18. Responsibilities arising from non-compliance with the policy

1. Objective

The purpose of this document is to establish the rules and principles that must be considered by WINDAR users during the use of technological means and resources and, in general, the information systems provided by the organization for the development of activities, in order to ensure adequate protection of the organization's information.

The information, whether our own or that of our clients, is a fundamental resource for the organization and requires adequate protection in order to ensure effective development of the organization's operations, and compliance with existing contractual and legal requirements in this regard, including those derived from the personal data protection regulations.

This information security regulation has been made based on the principles and commitments assumed by the management of WINDAR through the Information Security Policy that is approved and published through the organization's website.

This security regulation has been developed taking into consideration the main reference standards and norms (in particular, the ISO 27001 information security standard), as well as the needs derived from the contractual and legal requirements applicable to the organization (in particular, those derived from the personal data protection regulations).

This document will apply to all users who have access to the use of information systems owned by the company, including computer equipment (PC, laptops, servers), communications infrastructure, connection to internal or external networks, terminals, software, hardware, telematics services, network infrastructure, Internet access, non-automated media (paper), and, in general, all the resources to which the staff or user has access for the fulfillment of tasks assigned in the field labor.

2. Use of information

Information is an asset of transcendental importance for the organization and, therefore, requires adequate protection that reduces the risks associated with loss of confidentiality, integrity or availability of the same. To ensure this protection, WINDAR has developed this security regulation applicable to all users of the organization with access to information and processing systems.

In general, users must consider the following rules and guidelines:

- Access and use of information by users will be limited to what is strictly necessary for the effective performance of their professional activity, and no information may be accessed or used for which they do not have authorization, or that is not necessary for the development of their duties. tasks unless expressly authorized by those responsible for this purpose. In general, the principles of “least privilege” and “need to know” will be applied in the organization.
- Access to the organization's information will be controlled by the rules defined in the corresponding section of this report.
- In WINDAR there are different types of information of greater or lesser relevance or criticality, which will require the application of additional measures. In this sense, the existence of public or unrestricted information is considered, as well as confidential information or information subject to access restrictions or limitations, taking into account the importance of its confidentiality. Information classification and labeling mechanisms will be enabled from WINDAR in order to allow the user to know the type of information they are accessing and the additional security measures they must consider accordingly.
- El intercambio y almacenamiento de la información de WINDAR deberá de ajustarse igualmente a las sistemáticas y medios de almacenamiento e intercambio que se detallan en la presente normativa de seguridad.
- In general, WINDAR information must be treated by staff following the guidelines established through these regulations, and generally applying the necessary protection and care to it, taking into account the needs of confidentiality, integrity and availability of information and services.
- Access and use of information through the systems provided by the organization will comply with what is defined through these regulations, in the sections developed below.
- The exchange and storage of WINDAR information must also comply with the storage and exchange systems and means detailed in these security regulations.

3. Use of information systems & ICT resources

For the proper development of user activities, WINDAR will make available the necessary means and processing systems, and will enable the relevant access mechanisms to access and process the information it needs to carry out its functions. In general, the use of the computer systems made available to you must be subject to the following rules of use:

- The information systems and ICT resources provided to users belong to the company and their use must be used exclusively for work purposes, unless expressly authorized by management or those responsible for this purpose.
- It is the responsibility of the user, to the extent of their possibilities and with the collaboration of those responsible and the IT area, the care and good treatment of the assigned computer resources, following the standards and good practices defined through these regulations as well as other standards, policies or good practices that are formally communicated to you.
- The computers have a default security configuration defined by the designated WINDAR managers that responds to the needs of the organization to deal with threats that may affect it (this includes antivirus systems, access limitations, security updates, monitoring tools,...).
- Likewise, computer equipment is delivered to users with the applications, software and utilities they need to perform their functions, trying to limit unnecessary applications or functionalities that may increase the risks to the systems.
- The modification of this initial security configuration of the equipment, as well as the installation of additional software, is expressly prohibited without prior authorization from the corresponding managers, which must be carried out through the ticketing tool available for this purpose.
- Likewise, the installation of any additional software that is required by the user must be subject to prior authorization and validation by the corresponding managers and system administrators, which will be managed through the installation tool ticketing enabled for this purpose.
- In general, and except for duly justified exceptions, WINDAR will enable the necessary access control and assignment of appropriate privileges mechanisms to limit user permissions to modify the system configuration, requiring the corresponding authorization and participation of the users. system administrators.

- All WINDAR information must be stored and accessed centrally through the folder structure that is enabled or the management tools available in the organization for this purpose (CEDOC), which allows, among other aspects, adequate availability and accessibility, and the application of security measures in a consistent and centralized manner.
- Unless expressly authorized, it is forbidden to store information locally on computers, or on other media or storage media (USB devices, external media, cloud storage utilities such as Dropbox, Drive,...).
- Computer resources (user stations, portable servers, storage media, etc.) must be located and oriented in such a way as to minimize the possibility of unauthorized physical or visual access. WINDAR will enable the necessary mechanisms to ensure this correct location, and users must notify the corresponding managers in the event that they detect any deviation from this measure, so that the necessary corrective measures can be taken.
- Likewise, computer equipment must be located in such a way as to minimise the risks derived from physical threats (such as moisture, dirt, dust, blows or falls,...) or the impact that these threats may have on WINDAR's information or services. WINDAR will take this aspect into consideration at the time of installation of the equipment, although users must collaborate, as far as possible, in the application of this measure, notifying the corresponding managers in the event that any deviation is detected in this regard.
- WINDAR will develop the preventive or corrective maintenance processes necessary to ensure that the computer equipment is in the appropriate physical condition to ensure its correct operation, as well as to ensure that they maintain the necessary security configuration.
- To this end, WINDAR reserves the right to access the users' equipment at any time, by the system administrators and the persons responsible designated for this purpose, in order to ensure adequate maintenance of the equipment, according to the conditions defined in the corresponding section of these regulations.
- In general, the user will take all appropriate precautions and security measures to safeguard the material, content and information entrusted to him/her, including computers, magnetic or optical media or any device containing information from WINDAR.
- Users to whom these devices have been assigned must, to the extent of their responsibilities, properly guard these equipment, and adopt measures aimed at preventing damage or theft, as well as access to them by unauthorized persons.
- In this sense, actions must be taken into account such as not leaving equipment unattended when it is in customer facilities, or, in general, outside the organization's facilities, especially in areas where they can be accessed by unauthorized users.
- In the same way, actions should be taken such as not leaving mobile equipment or devices in sight when they are moved outside the offices or carried in vehicles, and measures and good practices should be applied aimed at minimizing their exposure, such as, for example, not keeping these devices in users' vehicles unnecessarily or indefinitely (for example, in transfers or movements outside the workplace).
- In cases where it must be left unattended, users should be sure to leave the equipment locked or turned off.
- In the event of theft or loss of equipment or devices, users must notify the support service as quickly as possible through the utilities provided for this purpose. When reporting the incident, the user must provide as many details of the incident as possible and must indicate the information that may be affected (either because it is stored on the computers themselves, or because it can be accessed through the utilities and applications installed on it).
- When the professional circumstances change (completion of a task, termination of the position, modification of permissions, etc.) that led to the delivery of a mobile computer resource, the device must be returned according to the deregistration procedure defined in the organization, which must be returned to the IT area, in order to proceed with the secure deletion of the stored information and restore the equipment to its original state so that it can be assigned to the computer a new user.

4. Prohibited, unlawful or unacceptable uses

The actions described below are strictly prohibited, or will not be considered acceptable by WINDAR's management, because they may involve illegal acts or that seriously jeopardize the organization's information or assets:

- Disclose information considered confidential, secret, or restricted to persons outside the organization, or to unauthorized persons, that may cause damage or harm to the company. Employees must maintain the utmost confidentiality regarding the information to which they may have access, especially the information of our customers, or that which contains personal data, for which they undertake to comply with the Confidentiality Agreement included in this document.
- In general, users may not access or make use of information that has not been granted authorisation or is strictly necessary for the development of the work activities entrusted to them. In the event that users detect a possible or potential access to information for which they do not have authorization, they must report it as an incident through the ticketing tool enabled for this purpose.
- Access to the Internet will be limited to those services or utilities strictly necessary for the development of our activities, and access for recreational, personal or extraneous (or incompatible) purposes to our activities will not be permitted, unless expressly authorized by the designated Controllers.
- It is forbidden to handle liquids, food, beverages near computer equipment, or carry out other actions that may directly or indirectly cause its malfunction, and the user is responsible for its deterioration.
- Altering, in whole or in part, the hardware, software and operating system configurations of computer equipment assigned to the same user or to other users, without proper authorization
- Attempt to access resources without authorization, through the use of intrusive tools, unauthorized cracking or use of passwords, exploitation of vulnerabilities, or any other unauthorized means.
- Failure to store with due diligence the keys, passwords, usernames or any other identifiers that may be provided to the employee to use any of the tools, or to access the Company's equipment or systems.

- Knowingly upload or introduce files that contain viruses, Trojan horses, worms, corrupted files, or similar software that may impair the operation of network equipment. Users should consider the guidelines or good practices that are transferred from the Organization to try to minimize this type of risk.
- Use network services in a manner that could damage, disable, overburden, or impair any other equipment or system of the organization.
- Connecting unauthorized computers to the organization's network, except in the exceptions and resources enabled by WINDAR for this purpose (e.g., use of guest WIFI)
- Send spam, indiscriminate, or chained mail, or unauthorized, or previously consented to by the recipients.
- Perform denial-of-service attacks that cause damage or disabling of the organization's information assets.
- Impersonate another user or entity or deceive or confuse about the origin of communications or other content for fraudulent or inappropriate purposes, or those that are not strictly necessary for the proper development of WINDAR's activities.
- Access to logs, traffic or access information, or the monitoring of any network or system, without these activities being carried out for purposes necessary for the developments carried out, or adjusting to the needs of the project.
- Any activity that attempts to collect information from any equipment or system for purposes not previously stated or agreed upon.
- Download software from the Internet or any other online service on any computer without prior authorization to do so, or without it being necessary for the development of the organization's activities.

5. Monitoring & verification of acceptable use

The inappropriate, abusive use, or the use that escapes the tolerated habits of communication services and technological means will be sanctioned with the elimination of access to resources, the application of disciplinary sanctions derived from non-compliance with the terms and conditions that emanate from the employment relationship, in addition to the legal sanctions established in the applicable current regulations.

The company may carry out the necessary investigations and controls of both the PCs and laptops, as well as the tools provided to the user by the company, which includes, among others, corporate email, tablet, smartphone or similar devices, etc., within the scope of the employer's powers of control under Article 20.3 of the Workers' Statute.

The control and access to the means provided by the company, including the documents generated by them and the communications that come from them, may be carried out without specific justification, temporarily or permanently, given the nature of said means as production tools provided by the company.

The control of these means will be carried out without harming or attacking the dignity or privacy of the user, given the knowledge that the user has of the object and the existence of the present control and supervision to which the users are subjected. The general purposes of this control are as follows:

- Protection of computer systems and network and the equipment that comprises it, in order to protect the integrity of the System and Information Security.
- Guarantee the continuity of work in the event that the user is absent due to illness, vacation or other similar reasons.
- Prevention of liability to third parties.
- Verification of compliance with the user's work obligations.
- Verification of the existence or not of an abusive or improper use of the technological means provided by the company, either for personal use, improper use or in general uses for which the user has not been duly authorized.

Therefore, all the contents, information and files stored therein, including temporary information, may be accessed by the company or by the persons designated for this purpose.

The scope of these control or inspection procedures shall be notified to all users in such a way that they are publicly recorded.

This document sets out a series of recommendations that regulate the proper use and availability of computer resources, and the company undertakes to disseminate them to all employees. Users who repeatedly, deliberately or negligently violate them will be subject to the technical or disciplinary actions deemed appropriate.

6. Information Sharing

For an adequate development of work activities, it may be necessary for users to exchange information both with internal users or collaborators, as well as with external users or parties. In order to ensure a secure exchange of information that reduces the risks that may arise from it, the following aspects must be taken into consideration:

- The use of e-mail and external media as means of exchanging information will be subject to the guidelines and standards
- WINDAR will enable the necessary mechanisms to enable a secure and effective exchange of information between both internal users and external users of the organization. Users must use these information exchange mechanisms, and must require express authorization in the event that they intend to use any additional mechanism.

  ⇒ In this sense, the exchange of information internally (between users of the organization) will be carried out through the internal utility (CEDOC), through the folder structure of the organization's server computers, through email (taking into account the indications made in the corresponding section) and the cloud services allowed by the organization (OneDrive and WCloud). In addition, WINDAR may consider and enable other additional mechanisms about which users will be informed in a timely manner.

  ⇒ The exchange of information with external users will be carried out through email (with the limitations set out in the corresponding section) and the cloud services allowed by the organization (OneDrive and WCloud). In addition, WINDAR may consider and enable other additional mechanisms about which users will be informed in a timely manner.

  ⇒ In the event that external users (customers, suppliers, collaborators,..) intend to share information with WINDAR users by means other than those indicated, the IT area or the persons responsible designated for this purpose will be consulted in order to evaluate the feasibility of using these tolos.

- In general, and unless expressly authorized, no storage, file synchronization programs, virtual hard drives or Internet backups such as Dropbox, Box, Google Drive, etc., may be installed and exploited to safeguard, share, or distribute information and data of the company or its customers, or any type of work documentation.
- In the event that the information exchanged or provided to external parties contains personal data or is categorized as confidential information or restricted use, the need to sign the corresponding confidentiality commitments or external data processing contracts must be considered. In case of doubts in this regard, the user may contact the persons designated for this purpose, through the ticketing tool.
- For adequate protection of confidential or restricted information, it may be necessary to apply additional measures such as encryption mechanisms or communication or exchange channels with adequate security protocols. WINDAR will provide users with the tools and mechanisms necessary for an adequate application of this measure.

7. Access Control Policy

As indicated, users should only have access to the information and resources that they strictly need for the development of their work activity. WINDAR has implemented the necessary processes and mechanisms to reduce the risks derived from unauthorized, excessive or inappropriate access. In this sense, it should be considered that:

- Each user will have a personalized account, equipped with the accesses and applications exclusively necessary for the correct development of their professional tasks. The user must not modify or violate the permissions provided by the company, especially with the intention of installing non-work-related applications.
- In the event that the user deems it appropriate to extend their permissions or install a specific application to carry out their work, they must request it from the responsible parties designated for this purpose, through a ticket or request generated for this purpose.
- All access to equipment and information systems shall be controlled and authorized by the system administrators or persons designated for this purpose. It is strictly forbidden for the user to attempt to access systems or resources to which they do not have express authorization from them.
- All authorised users have access to the computer systems by means of a personal and non-transferable username and password, undertaking to treat it with the utmost diligence and confidentiality, being solely responsible for the proper use of it. The authorized holder will be solely and directly responsible for everything executed in the system under his/her username and password. Repeated attempts, by any means, to gain access to other users' passwords without their consent are also strictly prohibited.
- At the time of registration with the company, the system administrators or managers designated for this purpose will provide the user with their access identifier and password in a secure manner, guaranteeing in all cases their confidentiality and secrecy, providing the user with the possibility of subsequently modifying the password.
- Access passwords will be subject to the strong password policies that are defined in order to ensure their effectiveness and protection, including aspects such as minimum length, use of complexity requirements (special characters, numbers, upper and lower case, etc.), expiration,....
- In general, it is forbidden to disclose by any means the access codes to any of the services provided to employees, except, exceptionally and justifiably, to system administrators or IT managers, for specific tasks of administration and/or resolution of incidents. In these cases, there must be a record of this exceptional use and the activities carried out in this regard.
- All usernames, passwords, access codes and other identifiers provided to the user will be confidential, personal and non-transferable, except with the exceptions indicated above. Users undertake to notify the system administrator and/or the security manager immediately of any incident or anomaly detected in access to the information systems or in their security.
- Users are responsible for the use and custody of the access codes or passwords assigned to them for the use of the company's computer equipment or services, and must not communicate them in any case to other users, nor record or write them in any format (whether digital or paper) except in those specific tools that are enabled in the organization and that guarantee their secure storage, in order to avoid unauthorized access to the systems, or that the user's identity can be impersonated.
- The user will not allow third parties to access WINDAR computers or systems using their credentials, except when explicitly authorized by WINDAR for the resolution of a problem.
- Each time the user finishes their working day, or is absent from their workstation, they will be responsible for blocking or closing their session on the WINDAR computers and systems to which they are connected.
- Periodic and scheduled reviews of users' access rights, privileges or permissions will be carried out by the Responsible Persons designated for this purpose, verifying that they have access to the utilities, resources or systems they need to carry out their functions, and that the principle of "least privilege" is complied with.

8. Email Usage Policy

E-mail is a tool that the company enables for those communications required as a result of the development of the company's own activity with other entities or with other users. Access to and use of these services by users, as well as the privileges associated with this right, must be limited to those established by their professional obligations. WINDAR, aware of the security and legal liability problems caused by the use of e-mail, has the following rules:

- Business e-mail, distribution lists, instant messaging services and other electronic communication services are tools whose main objective is to facilitate corporate communication exclusively in the workplace.
- Users will be responsible for all activities carried out with the access accounts and their respective mailbox provided by the company. Users should be aware of the risks involved in the misuse of e-mail addresses provided by the company and the possible repercussions (such as damage to the company's image) that could result from the improper use of such resources.

- Communication tools should not be used for personal use, nor may personal email accounts, based on web access, such as gmail, hotmail, be used. Exceptionally, it may be used only when the situation is duly justified and does not contravene the interests of the company in any way. In this case, access must be exclusively to those emails that are fully trustworthy, and in no case should links be opened or attachments downloaded to the user's or other users' computers, even if they come from known people, in order to avoid the intrusion of viruses or malicious code.
- It is strictly forbidden to forward emails and work documentation to personal email accounts, or those that are not under the direct control of the company, as well as the redirection, import or download of corporate email to other webmail managers or platforms such as Gmail, Hotmail, etc.
- The form and content of the emails sent by the user will be aligned with the ethical and courtesy standards set by the company, and in no case will emails be sent with offensive, threatening, distasteful, illicit or fraudulent messages. All messages sent by corporate email must include the legal notices, format, contact information, and other information that makes up the signature models of the corporate emails that are indicated to users by the designated managers during the registration process in the company.
- It is forbidden to use e-mail for profit or commercial purposes, for recreational use or any other that is not related to work activity, or that is unrelated to the development of the company's own activities.
- It is forbidden to use professional mail to subscribe to newsletters, news groups, or similar that are not directly related to the professional activity carried out by the user and that are of full trust.
- Mailing lists may only be used for the company's own purposes, and never for advertising, commercial or personal purposes that are not related to work performance.
- Emails that reveal data from the directory or users belonging to the company, outside the work limits established by the company, will not be disclosed, regardless of the format in which they are found.
- The personal corporate email account and the corporate signature will be the only ones authorized for use in personal communication with third parties (customers, suppliers, partners, etc.). etc.).
- Users will need to do due diligence in the address bar before sending a message. Sending information to the wrong recipients can result in a breach in the confidentiality of the information. When replying to a message, it is important to review the addresses listed in the Copied (CC) field.
- Emails should not be sent or forwarded in bulk. If an email is sent to a group of recipients, it is advisable to use a distribution list or, failing that, place the address list in the Blind Copy (BCC) field, preventing its visibility to all recipients of the message.
- Do not send chain messages. Virus alarms and message chains are, in many cases, simulated emails, which aim to saturate the servers and the network. If you receive a chain message alerting you to a virus, you should delete it immediately.
- Do not respond to spam messages. Most spam message generators are sent to randomly generated email addresses, hoping that the responses obtained will confirm the existence of real account addresses. In addition, they sometimes have the appearance of legitimate messages and may even contain information relating to the Organization. In any case, they should never be answered.
- In general, it is not authorized to send emails that contain information with confidential or restricted use data in the body or in the attachments, and the use of other types of tools available in the organization (indicated in the Information Exchange section of this document) must be prioritized. If it is necessary to send this information, you must contact the persons responsible designated for this purpose, through the ticketing tool, who will provide you with alternative mechanisms to do so.
- Secure the identity of the sender before opening a message. Many cyberattacks originate when the attacker impersonates a known person or entity (friend, colleague, etc.) of the person being targeted. The origin of these actions is diverse: unauthorized access to the account, visual impersonation, introduction of malicious code that uses the sender account to spread, etc. In case of receiving a suspicious email, and depending on its plausibility, it is possible to: ignore it, do not open it and inform the sender of the fact, regardless of reporting the corresponding security incident. Similarly, the sending of confidential or restricted information at the request of an email whose identity cannot be assured of the sender should be rejected. It is important to note that it is very easy to send an email with a fake sender. You should never trust that the person you communicate with via email is who they say they are, except in those cases where electronic signature mechanisms are used for emails (not just attachments).
- Do not open junk or suspicious emails. Even if an unwanted message has passed through the spam filter, it should not be opened, and the corresponding security incident should be reported. It's a good idea to delete suspicious emails, or at least place them (unopened) in a quarantine zone.
- Do not run suspicious attachments. Received attachments should not be executed without first being scanned with the anti-malware tools available in the organization, which will be configured to perform this scan automatically. This is especially important when unsolicited attachments are received or the mail is suspicious. Much of the malicious code is usually inserted into attachments, either in the form of executables (.exe, for example) or in the form of application macros (Word, Excel, etc.).
- Report emails with viruses, without forwarding them. If staff detect that an email contains a virus or, in general, malicious code, the IT area must be notified of the security incident and not forwarded, to prevent its possible spread.
- Do not use email as storage space. Space capacity on mail servers is limited. When an account becomes saturated, the server may restrict the privileges of sending and/or receiving messages or carry out a more or less selective deletion of the stored messages. For all these reasons, it is recommended to keep only essential messages and periodically review those that have become obsolete. In this sense, the organization will develop rules and policies for the elimination of information, which will be communicated to users for consideration and application.
- WINDAR reserves the right to access and monitor the use of this and any other resource provided to users, as long as this access is legitimized or justified to ensure the continuity of the company's operations and the provision of services, guarantee or supervise the security of information and the application of the procedures defined in this regard, or ensure the performance of workers, always taking into account the provisions of the Workers' Statute and the rest of the applicable legislation, and as indicated in the corresponding section of these regulations.

9. Policy for the Use of External Media

The use of external media, such as USB sticks, external hard drives, CDs/DVDs,... It may be necessary in the organization to carry out certain tasks such as the transfer of information or its exchange with customers or other parties, information backup, exchange of information between areas, etc. However, its uncontrolled use can introduce information security risks such as dispersion and loss of control of information, loss of information, unauthorized access, introduction of viruses into the organization's systems, etc. For this reason, WINDAR has defined the following rules of use that must be applied by all users in the organization who use or can use external media:

- In general, the use of external media by users is prohibited unless expressly authorised by the responsible parties designated for this purpose, for their use for specific purposes associated with their work activity, such as the exchange of information with customers or internal users. In this sense, it will be a matter of prioritizing other tools available in the organization for the exchange of information, such as those indicated in the corresponding section of these regulations.
- In any case, the use of media will be limited to professional purposes, and its use or connection to the organization's systems for personal or other purposes is prohibited.
- The authorisation for the use of media will be managed through the ticketing tool enabled for this purpose, and will be carried out by the managers designated for this purpose (area managers), under the supervision of the IT managers, who will be responsible for managing the custody and assignment of the authorised supports, maintaining the corresponding inventories of supports and records of their assignment.
- Only the use of corporate supports, managed and controlled by the corresponding managers of the organization, is authorized. The use of personal or non-organizationally controlled removable media is prohibited.
- The use of external media provided by customers, collaborators, suppliers and other third parties to exchange information with WINDAR must also be subject to the authorization and supervision of the designated managers and IT staff, who will be responsible for validating and authorizing their use and evaluating the risks that they may introduce on WINDAR's systems.
- Once the users finish the tasks for which they required the use of media, they will be returned to the corresponding responsible parties so that the information contained therein can be safely deleted and verified that they are free of malicious code.
- In general, and especially in the event that confidential information or information for internal use is stored therein, external media must be encrypted through the mechanisms that the organization will enable for this purpose.
- The organization may implement the necessary technical measures to monitor the use of removable media and/or to limit and block its use according to the needs of the organization and in order to guarantee the security of its own or our customers' information.
- During its use, users must apply, as far as possible, the good practices and uses necessary to avoid incidents that affect the security of the information such as unauthorized access, loss of information, introduction of viruses and malicious code, etc.
- In the event that users suffer or detect any incident related to the use of media, or to compliance with these regulations, they must notify the IT area through the established incident notification mechanisms.

10. Responsible use of the internet. Navigation restrictions

The Internet is a service that WINDAR makes available to its staff for strictly professional use. The company is aware that the introduction of the Internet in the workplace increases threats to network security, affects employee productivity and decreases available bandwidth. Therefore, it considers itself obliged to establish the following rules that must be applied during its use:

- It is forbidden to use the network to browse Internet sites for uses other than those permitted for the performance of their work activity, unless expressly authorized to this effect.
- Users are solely responsible for the sessions initiated on the Internet from their work terminals, and undertake to comply with the rules and operating standards set forth herein.
- Browsing websites, sending messages, registering, registering, filling in forms and any other activity carried out via the Internet, will be the full responsibility of the sending user and in any case must assume the consequences arising from their actions.
- If you have any doubts regarding the possible uses of navigation and the aspects indicated above, you can contact the support area through the corresponding ticket or support request.
- Access to the company's Internet service by external personnel will be carried out in a controlled and authorized manner, and the information defined in the visit management process defined in this regard must be followed.
- The company reserves the right to filter the content that the user may access through the Internet from the resources and services owned by WINDAR, as well as to monitor and record the accesses made from them.
- In the event that users require access to web services that are blocked or limited by the organization, the corresponding authorization must be obtained from the area managers, and the corresponding request must be generated to the IT area, through the ticketing tool enabled for this purpose, who will evaluate the feasibility and possibility of facilitating access according to the needs of the user and the organization and the risks that may arise from them.
- It is strictly forbidden to access, download and/or store on any medium pages with illicit, harmful content, pornographic material, xenophobic, racist, sexual content, or any inappropriate material or material that violates dignity and ethical and moral principles, and, in general, any type of content that does not comply with the company's rules of courtesy.
- It is also not allowed to store files and personal content downloaded via the Internet on computers, especially those that violate current legislation on intellectual property. Users must respect and comply with the legal provisions on intellectual property rights.

11. Use of Software Licenses

The software or applications used by the organization, as well as other information resources, may be protected by intellectual property, or have copyrights or copyrights. WINDAR has the necessary tools and systems to ensure effective compliance with these requirements. In this sense, users should consider that:

- Users are obliged to respect the license and copyright conditions of the software installed on the computer equipment, being responsible for its proper use.
- Any copyrighted software may not be copied, nor may any copyrighted information in electronic form be made available on any user's computer.
- Users may not install or download software without the prior authorization of the persons responsible designated for this purpose, who must ensure proper compliance with the legislation related to intellectual property. Software may only be installed on the organization's systems that is duly authorized and complies with the requirements of the Intellectual Property Law.
- Users will be responsible for any software installed on their equipment without express authorisation from the responsible parties designated for this purpose, as well as for the use and, where appropriate, for any damage caused to the equipment or information systems resulting from its use or installation.
- Any activity that violates intellectual property laws, including copyrights, trademarks or registered rights and their reproduction will be sanctioned as indicated in these regulations.

12. Processing of personal data

WINDAR has implemented the necessary mechanisms to ensure adequate compliance with personal data protection regulations. In general, the organization will provide users with the necessary tools and procedures to ensure effective compliance with these regulations. However, they may occur during interaction with customers, suppliers, collaborators and other interested parties, situations in which the participation of WINDAR users or employees is necessary. In this regard, WINDAR has appointed specific persons responsible for compliance with data protection regulations (in particular, a Data Protection Officer has been appointed) who are available to the organisation's employees to guide, advise or clarify any doubts that may arise regarding compliance with the requirements of the regulations. In this sense, users should be aware that:

- The processing of personal data must respond to a legitimate and specific purpose, such as, in general, the maintenance of a contractual relationship (such as that maintained with customers).
- The personal data used during the development of internal or external services must be proportionate to the purpose of the processing, and no more data than those that are strictly necessary to comply with said purpose must be used.
- Data subjects have the right to be informed about the processing of their data, as well as subsequent access to them, and their cancellation, rectification, opposition, portability or limitation of processing. In the event that any affected party addresses the users of the organization directly for the exercise of the indicated rights, the user must transfer, as quickly as possible, this request to the responsible parties designated for this purpose.
- Personal data must be adequately protected, for which the measures indicated in these regulations will apply, among others. Additionally, depending on the type of data and the purpose of the processing, it may be necessary to apply additional measures such as the application of encryption, pseudonymization or anonymization of data mechanisms, for which WINDAR will enable the necessary tools and mechanisms.
- Incidents or security breaches affecting personal data must be reported (according to the mechanisms set up for this purpose) as quickly as possible, in order to respond to the requirements of the regulations in this regard.
- Access to personal data by third parties must be regulated through the corresponding external data processing contracts. WINDAR has the appropriate procedures for the establishment of such agreements, although users, when they intend to exchange or send information containing personal data, must consult and verify the existence of such agreements, requesting or consulting the Data Protection area of Windar through the means of contact enabled for this purpose.

13. Incident Management

All incidents in the use of the company's technological resources and means, or that, due to any circumstance, direct or indirect, may compromise Information Security, must be notified as soon as possible through the means enabled for this purpose.

In this sense, WINDAR has a ticketing tool (GLPI) through which, among other aspects, incidents that affect information security, processing systems and ICT resources are managed.

In general, users should prioritise the use of this tool for reporting incidents, although, exceptionally, and especially in the event that access to this tool is not available, incidents may be reported by email or telephone, by contacting the persons designated for this purpose.

In the notification of the incident, the user must transfer as much information as possible about it, trying to indicate aspects such as: the description of the incident, its origin, the affected assets, the affected information, as well as other information that may be considered relevant.

WINDAR has designated the managers and specialized personnel necessary for an adequate management of the incidents after their notification, who will be in charge of carrying out the diagnosis, monitoring and resolution, keeping the incident register updated throughout the process, and, where necessary, keeping users informed about it. During this process, it is possible that the designated managers and technicians may require additional information from the user in order to try to optimize the resolution of the same.

14. Use of corporate mobile phones

In order to optimize and facilitate the work of its employees, WINDAR offers telephony and data solutions to users who, due to their skills, need them. However, the fraudulent use of the telephone, landline or mobile, can jeopardize the integrity of the company and harm its interests. This can happen through the practice of activities considered illegal, that violate ethics or morals or may be offensive, or even as a result of the abusive use of it.

Mobile phones and USB 3/4G data modems are assigned to WINDAR users and collaborators who, within the scope of their professional activity, need to make or receive frequent and regular contacts with customers, suppliers, collaborators and coordinators, or must travel outside the company's permanent offices, and/or must be located for reasons of their work (commercial, consulting, maintenance, etc.).

Each manager of the operational area, project or service must determine the interest in the use by the respective collaborator of a mobile phone, smartphone or USB 3/4G data modem. In the event that the proposal is approved by the management of WINDAR, the director of the operational area will request the managers designated for this purpose to begin the procedures for the contracting of the necessary equipment.

The general terms and conditions of use of this service are as follows:

- The mobile phones, smartphones, USB 3/4G data modems, provided by the organization, as well as all their accessories, and the corresponding network service contract, are the property of WINDAR and their use must be in accordance with the rules indicated in this document, as well as in other policies or regulations that may be developed for this purpose
- For logistical and control reasons, the contract of the relevant network operator is nominal to WINDAR.
- Personal use of telephone communications will be permitted if it is incidental or insignificant, and does not interfere with normal work activities or impair the performance of such activities.
- In the event of a collaborator/employee's resignation from the company, he/she must return the terminal, including its original packaging, in perfect working condition, and may have the possibility of acquiring the terminal for its residual value, if applicable. Once the device has been returned, WINDAR will proceed to delete all data and information from the cell phone (including contact list, photos, messages, etc.). in order to enable their reassignment or safe retirement.
- The professional use of the mobile phone equipment will focus on the best quality of service to our customers, on the improvement of the quality of reaction, and therefore on the increase in productivity of the WINDAR collaborator.
- It is the responsibility of the WINDAR collaborator to make the best professional use of the mobile phone equipment.
- Under no circumstances will WINDAR finance the purchase of accessories (hands-free kits, cases, data transmission kits, etc.) or their installation. The collaborator is directly responsible for any damage that may occur in the assigned terminal due to the use of these accessories.
- WINDAR may at any time request the return of the terminal in whole or in part to the collaborator, who must return it in perfect condition.

WINDAR reserves the right to review the list of voice and data calls made, to verify compliance and follow up on the rules in the event of any well-founded suspicion or evidence of fraudulent or abusive use of the service, as well as to withdraw the right to use the mobile phone/data modem in case of inappropriate use, abusive, and/or that causes damage to the company.

The company reserves the right to modify these regulations as the scope of application thereof, after notifying its collaborators.

15. Organization of Security of Information

WINDAR has defined the responsibilities necessary for an adequate management of information security, as well as, in particular, to ensure an effective performance of the aspects defined in this regulation. In particular, an Information Security Committee has been set up at WINDAR with the responsibility of coordinating, centralizing and managing the processes necessary for proper information security management and decision-making.

In relation to the provisions of these regulations, the Security Committee is available to users to offer the necessary support and advice for the aspects indicated in these regulations, including those aspects for which users require clarification or additional guidance.

Communication with the Security Committee will be carried out, in general, through the ticketing tool (GLPI) where a specific categorization has been established for aspects related to information security.

In particular, the heads that make up the Safety Committee, and who are available to users to offer the necessary support and advice, are:

⇒ Raúl González, Management system responsible
⇒ Covadonga Carballo, Technology and Innovation Director
⇒ Fernando Ruiz, IT Responsible
⇒ Oier Zurimendi Unzueta, Data Protection Responsible (DPO)

On the other hand, WINDAR will develop the necessary awareness and training activities to ensure that all users of the organization have a level of awareness and training in information security appropriate to the needs associated with their position or job profile, in order to reduce the information security risks that may arise from their activities.

These training and awareness-raising actions will be governed by what is defined in the training procedure, and will be aimed at fulfilling, among others, the following objectives:

- Adaptation to new technologies and new work systems
- Increasing the qualification of staff
- Compliance with the rules and policies defined by the organization
- The importance of compliance with information security and software quality policy, procedures, and requirements,
- The information security risks associated with your work,
- Their roles and responsibilities in achieving compliance with safety requirements,
- The potential consequences of deviating from the procedures that apply to them,
- The importance of their participation in the process of continuous improvement of the Information Security and Software Quality Management System.
- The importance of the duty of secrecy and the commitment to confidentiality assumed.

These training and awareness-raising actions may include, among other activities:

- Communication of security policies and regulations,
- Specific internal or external training actions,
- Internal awareness-raising talks,
- Communications by e-mail, intrantet or other means of communication of good information security practices or information about system vulnerabilities and threats that may affect you,
- The development of controlled or simulated phishing exercises,
- The development of tests or surveys that allow the organization to evaluate the degree of awareness and awareness in terms of information security.

16. Control and Monitoring Programs and Devices

WINDAR has put in place automated control tools and services to analyse and detect those events that may pose risks to the security of information and systems or to identify improper or illicit uses and behaviours on the network, such control not involving a violation of the privacy or intimacy of users. and being carried out, in any case, respecting the rights set out in the labour regulations (Workers' Statute).

WINDAR informs that, for security reasons, all the information that circulates through the network, as well as the email of the accounts managed by the company, may be monitored and subject to controls and reports on its use, providing information such as: user, date of accesses, time of accesses, bytes transferred, file storage, etc. access to servers, sites visited, time spent browsing the web, among others.

17. Use of Artificial Intelligence

WINDAR has authorized Microsoft COPILOT as an artificial intelligence assistant in the corporate environment. Other assistants available on the market, such as ChatGPT, Gemini AI, and others, are not authorized for use in the corporate work environment. The regulation of the use of these types of tools is primarily due to the risks their use entails for the confidentiality of information, as well as the safeguarding of rights related to personal data.

- Corporate environment refers to the internal work environment within the companies and locations of the WINDAR Group. It is characterized by the use of Microsoft COPILOT as an AI assistant through the acquisition of an official Microsoft license. This allows it to integrate with Office 365 tools, improving user productivity and ensuring greater security and privacy when using both your own and third-party documents.

  Use of the corporate environment will only be available to users authorized by the managers of each area or department. To do so, they must first request the corresponding license from the IT department.

- The NON-corporate environment refers to the use of COPILOT, as well as other artificial intelligence tools such as ChatGPT, Gemini AI, or others, openly, through an internet browser. The use of WINDAR's corporate data and information, as well as information belonging to clients or third parties, through these AI tools is strictly prohibited.

Security and privacy are crucial aspects in the implementation and use of artificial intelligence (AI) assistants. Therefore, all individuals at WINDAR companies and sites using AI assistants will ensure compliance with the following standards:

- They will be aware that they are communicating or interacting with artificial intelligence systems and will therefore be responsible for the appropriate and proper use of AI assistants.
- They will always use AI assistants that have been authorized by WINDAR and exclusively to assist them in the performance of their functions and tasks, always respecting the regulations, standards, and internal guidelines established by the company.
- They will always adopt principles of transparency and fairness, ensuring at all times the fair and beneficial use of AI assistants and the results provided by AI.
- They will act responsibly when using AI assistants, always applying the best available practices to minimize the risks associated with the automation of tasks and results.
- They will guarantee the privacy and security of the data and information used to power AI assistants. Under no circumstances will the AI be given access to sensitive and personal information. They will ensure the accuracy and veracity of the data and information provided by validating it prior to use.
- They will review the results with caution, especially if the data and information are used for decision-making.
- They will monitor the responses provided by the AI to identify and mitigate potential biases in the generated results, often due to the information provided by the user.
- They will interpret the results provided by the AI within the framework of their specific roles and tasks and, when necessary, will supplement them with their own knowledge or additional information.
- The responsibility for creating summaries, documents, or data analysis will never be delegated to the AI assistants. It is the responsibility of all WINDAR staff to verify the results and ultimately enhance them with their input.
- They will understand how the AI assistants work, the data sources to be used, and the limitations on their use. Internally established controls and policies to oversee their use will always be followed. Automated decisions will be prevented from being made without human supervision.

The IT department may conduct periodic audits and monitoring of AI use in order to detect early misuse of AI systems, which may lead to disciplinary action, within the applicable regulatory framework, where applicable.

18. Responsabilidades derivadas del incumplimiento de la normativa

This document is governed by Spanish laws and regulations, as well as those of the European Union and the autonomous communities regarding personal data protection, intellectual property, and the use of telematic tools, as well as applicable labor regulations and any other regulations that may arise in the future.

The user must be aware that failure to comply with these security regulations may cause significant damage to the organization and constitute a violation of their confidentiality commitment as an employee or user of WINDAR.

Users undertake to comply with these regulations to the extent possible and to notify the designated responsible parties if they detect or anticipate any breach. WINDAR may hold the user liable for the consequences arising from failure to comply with the regulations established in this document.

The company reserves the right to periodically assess compliance with this regulation (including through the use of automated control, auditing, and monitoring tools and services to analyze and detect events that may pose risks to the security of information and systems or identify improper or illegal uses and behaviors on the network) and to apply any disciplinary and legal measures it deems appropriate as a result of noncompliance.

If any action contrary to the provisions of this organization's security regulation or, as a last resort, a security breach is detected, WINDAR may order an investigation to determine the type of violation committed, evaluating the situation taking into account the following factors:

1. The nature and severity of the violation.
2. The impact of the violation on the organization's activities.
3. The level of noncompliance with safety regulations and the organization's culture.
4. The recurrence of proven facts.
5. The employee's skill and knowledge.
6. Other applicable legal factors.

The determination of the seriousness of the violation will take into consideration these factors, as well as the provisions of the Collective Agreement, the Workers' Statute, and any other applicable legislation.

If the violation is determined to be a minor violation, appropriate measures will be taken to correct the situation. This means the employee will be trained and provided with additional resources to develop the necessary skills and prevent future violations. Progress will be monitored to ensure that corrective measures are effective.

If the offense is repeated, warning measures will be taken, notifying the employee of the offense and reminding them of the corrective measures to be taken; if the offense persists, it will be considered a serious offense in accordance with the applicable legal or conventional disciplinary regulations, and the legal or conventional disciplinary regime will be applied in a manner consistent with the greater seriousness of the infraction.

If the breach is considered a serious or very serious offense, WINDAR may request the withdrawal of all access to information systems and facilities, as well as the return of assigned assets. Additionally, the corresponding areas of WINDAR will be notified to assess the application of the legal or conventional disciplinary regime in accordance with the greater severity of the violation, including among the possible sanctions the temporary suspension of employment and salary or disciplinary dismissal, depending on the severity of the violation. Although, as indicated, determining the severity of the offense will require WINDAR to analyze the different factors indicated, as a guide and without prejudice to the applicable legal or conventional disciplinary regulations, it can be considered that, in general:

⇒ The non-application or failure to comply with the guidelines defined in the Safety Regulations will be considered a Minor Offense, unless this non-compliance is carried out repeatedly or consciously, and can be considered an act of disobedience that may be classified as a serious or very serious offense.

⇒ The repetition of Minor Offenses, as well as the deliberate failure to comply with the Prohibited, Illegal, or Unacceptable Uses expressly defined in Section 4 of these Regulations, will be considered a Serious Offense.

⇒ A Very Serious Offense will be considered to be any serious offense that is committed repeatedly or can be considered a clear act of indiscipline or breach of good faith in the contract, or that seeks to deliberately cause damage to the organization's systems, without prejudice to the results of the application of the legal or conventional disciplinary regime applicable in general terms in the classification of very serious offenses.