POLICY FOR THE MANAGEMENT OF THE INTERNAL INFORMATION AND WHISTLEBLOWER PROTECTION SYSTEM

WINDAR
renovables

Issued by: System Manager	*Date:* xx/06/2023
Reviewed by: Management	*Date:* xx/06/2023
Approved by: Governing Body	*Date:* xx/06/2023

VERSION CONTROL HISTORY

Version	Description	Date
1.0	Initial version of the document	June 2023

Index

1. INTRODUCTION

The 2010 reform of the Criminal Code incorporated into the punitive text the criminal liability of legal people as a key institution for corporate crime prevention. In 2015, the possibility of exemption or attenuation of such liability in the event of the adoption of effective organizational and management models for the prevention of crimes was introduced, and with it was provided as an inexcusable requirement that such models establish "the obligation to report possible risks and breaches to the body responsible for monitoring the operation and observance of the prevention model" (art. 31 bis 5 paragraph 4, of the *Organic Law 10/1995, of November 23, 1995, of the Criminal Code*).

WINDAR's Code of Conduct sets out the corporate values and management principles that should guide the behavior of its members, internally and in their relationship with the organization's stakeholders. In the above-mentioned document, in the communication section, the obligation to immediately report any possible non-compliance is mentioned.

With the approval of *Law 2/2023, of February 20, regulating the protection of people who report regulatory infringements and the fight against corruption,* organizations must promote the implementation of whistleblowing channels or Internal Information Systems.

The Internal Reporting System is a fundamental measure for the prevention and detection of conduct contrary to the law and the organization's internal regulations. Furthermore, in addition to complying with regulatory requirements, it contributes to promoting good corporate governance, creating a labor climate of trust and providing organizations with greater transparency in their management.

2. OBJECT

In accordance with current legislation, WINDAR RENOVABLES, S.A.U. (hereinafter "WINDAR" or the "organization") enables this Policy for the management of the Internal Information System and whistleblower protection (hereinafter the "Policy") for the prevention and detection of behaviors contrary to the laws and internal regulations of the organization, as well as the protection of people who report these behaviors through the internal channels enabled.

The purpose of this Policy is to make available to all members of WINDAR and its Business Group, and to any third parties who have a professional relationship with the organization, an effective and easily accessible Internal Reporting System through which to communicate confidentially or anonymously irregular facts related to the entity.

This Policy has been drawn up as a result of the organization's desire to ensure an effective system for managing, investigating and responding to communications sent through internal communication channels.

3. SCOPE

This Policy defines the operation and principles governing WINDAR's Internal Reporting System, as well as the procedure for receiving, managing information, investigating and resolving cases, and applies to all communications submitted, as a result of the alleged commission of irregularities or unlawful conduct, to

through the internal channels provided and sent by all those who have obtained information on violations in a work or professional context, in accordance with the provisions of *Law 2/2023, of February 20, regulating the protection of people who report regulatory violations and the fight against corruption.*

All WINDAR members undertake to report any irregularity or unlawful behavior of which they are aware or of which they have well-founded indications, as provided for in paragraph 4 of Article 31 bis.5 of the Criminal Code.

4. DEFINITIONS

- ***Informant or whistleblower***: a person who reports an irregularity or illicit behavior, whether active or omissive, through the whistleblowing channels enabled in WINDAR's Internal Information System, in accordance with the provisions of Article 3 of *Law 2/2023, of February 20, regulating the protection of people who report regulatory violations and the fight against corruption*, shall be considered informants those people who have obtained information on violations in a labor or professional context, including in any case:

i. people having the status of public employees or employees of others;
ii. the self-employed;
iii. shareholders, participants and people belonging to the organization's administrative, management or supervisory body, including non-executive members;
iv. any person working for or under the supervision and direction of contractors, subcontractors and suppliers; and
v. those who communicate or publicly disclose information on violations obtained in the framework of an employment relationship that has already ended, volunteers, interns, trainees, workers in training periods regardless of whether or not they receive remuneration, as well as those whose employment relationship has not yet begun, in cases where the information on violations has been obtained during the selection process or pre-contractual negotiation.

- ***Person alleged to have infringed or reported***: person who is accused of an alleged violation of the legislation in force and/or WINDAR's internal regulations.

- ***Irregularity or unlawful behavior***: any act or omission likely to violate WINDAR's internal rules or, pursuant to Article 2 of *Law 2/2023 of 20 February, regulating the protection of people reporting regulatory violations and anti-corruption*, any act or omission likely to constitute breaches of European Union law, criminal offenses, serious or very serious administrative offenses and labor violations in the field of occupational safety and health. The scope of these irregularities or unlawful behaviors shall be understood without any geographical limitation. Events related to human resources policies (remuneration, professional development, vacations, etc.) or professional performance, among others, shall not be considered as such.

- ***Communication or denunciation***: information on the facts allegedly committed that constitute an irregularity or unlawful behavior.

5. RESPONSIBILITIES

The Head of the Internal Reporting System is the WINDAR collegiate body responsible for receiving communications, deciding on the merits or rejection of complaints, designating the body in charge of investigating the facts reported and deciding on the facts that are considered proven.

In the event that any of the accused people is a member of this collegiate body, the person concerned shall disclose this fact and withdraw from the procedure and, in the event that he/she is merely read, the informant shall be informed of this fact.

Likewise, the members of this body shall undertake to abstain from those investigations in which they may be involved or personally related to any of the people under investigation.

Pursuant to the provisions of Article 8 of *Law 2/2023 of February 20, regulating the protection of people who report regulatory violations and the fight against corruption*, WINDAR's management body has appointed a collegiate body as Head of the Internal Information System, which will consist of the people occupying the Corporate Human Resources Management, the Financial Management, the Secretary of the Board of Directors and the Legal Department Management, delegating to the latter the powers of management of WINDAR's Internal Information System.

The Head of the Internal Information System shall report directly to WINDAR's governing and/or administrative body and shall exercise his/her position independently of the aforementioned bodies.

The System Manager will be in charge of keeping a log book with all the communications received and the investigations carried out, guaranteeing at all times the minimum confidentiality requirements with respect to the data contained therein. Said log-book shall be of restricted access and shall only be disclosed at the request of a competent judicial authority within the framework of a judicial proceeding.

If deemed appropriate, the Head of the Internal Information System may appoint a body in charge of carrying out the investigation phase of the reported facts (hereinafter referred to as the "investigation body"). It shall be composed of at least two people, appointed by the Head of the System, from among its members and/or other people external to it, provided that they are not involved in the alleged facts reported and their intervention contributes to the best clarification of the information reported on the basis of their experience and/or knowledge.

The people comprising the research body shall sign a confidentiality agreement at the time of its constitution and shall be subject to the guiding principles of this Policy.

Its functions include investigating the facts and gathering the necessary evidence to support the results of its investigation, documenting the actions taken, preparing a report on the investigation and providing support to the System Manager in the other functions entrusted to it.

6. MANAGEMENT PROCEDURE

6.1. Guiding Principles

All communications sent through WINDAR's Internal Information System will be handled in accordance with the following principles:

- *Independence*: the communications received will be managed by the Head of the Internal Information System with full autonomy in his decisions, who will have all the personal and material means necessary for the exercise of his functions without being subject to the authority of the governing and administrative bodies.

- *Authority***:** The person in charge of the Internal Information System has the necessary competence and authority to manage communications, process investigation files and carry out all actions required by this Policy.

- *Objectivity*: the person in charge of the Internal Information System and the body in charge of investigating complaints shall act and make a reasoned decision, avoiding any type of arbitrariness in their actions and guaranteeing full compliance with the provisions of this Policy.

- *Confidentiality and privacy*: the receipt of the communication, the access to its content by all those authorized to do so, as well as the subsequent investigation and instruction of the file, will be carried out in a discreet and absolutely confidential manner, preserving the identity of all people affected by the information provided and ensuring compliance with national and Community regulations regarding the protection of personal data.

- *Anonymity*: under the provisions of Article 7.3 of *Law 2/2023 of 20 February, regulating the protection of people who report regulatory infringements and anti-corruption and* Article 24 of *Organic Law 3/2018 of 5 December on the Protection of Personal Data and guarantee of digital rights*, WINDAR declares anonymous communications lawful. The investigation and instruction of the process under an anonymous complaint, will be made ex officio with all the precise guarantees so as not to jeopardize the possible identification.

- *Prohibition of retaliation:* in no case will any retaliation be taken against people who report in good faith and with reasonable suspicion a possible irregularity or illegal behavior, except for the possibility of adopting a sanction, in a reasoned manner, based on the provisions of the applicable labor regulations, against those people who make false or misleading accusations, with intent to harm. Likewise, depending on the circumstances, it would be possible to mitigate or exempt from liability those people who, being related to or participating in the occurrence of the irregularity or illicit behavior, inform the Head of the Internal Information System and/or collaborate in the investigation, provided that the corresponding sanctioning procedure has not yet been initiated.

- *Presumption of innocence*: the presumption of innocence, the right of defense and the safeguarding of the right to honor of the people denounced, who shall have the right to be informed of the actions or omissions allegedly attributed to them and to be heard at any time.

6.2. Communication

6.2.1. Means of reporting

In order to create an accessible and effective Internal Reporting System, WINDAR has set up an online form for the communication of any irregularity or illicit behavior at the following url: https://compliance.materh.com/windar.

The processing of communications received through this channel will guarantee the anonymity of the user's identity through the use of a secure line that does not require prior registration or identification.

In addition to the internal online whistleblowing channel, which is of preferential use, WINDAR also makes the following channels available to informants for reporting irregularities or unlawful behavior:

- By e-mail to the following address: canaldenuncias@windar-renovables.com
- By mail to the address Parque Empresarial Principado de Asturias, Avda. de la Siderurgia 28, 2º, 33490 - Avilés (Principado de Asturias), to the attention of the person in charge of the Internal Information System.
- At the request of the informant, in person or by videoconference, by calling a meeting with the person in charge of the Internal Information System.

WINDAR has enabled the aforementioned internal online whistleblower channel to report violations in the prevention of workplace harassment, sexual and gender-based harassment, in accordance with the provisions of the Protocol for action and prevention of sexual and gender-based harassment, in compliance with Article 12 of Organic Law 10/2022, of September 6, on the comprehensive guarantee of sexual freedom.

Pursuant to the provisions of Article 25 of *Law 2/2023, of February 20, regulating the protection of people who report regulatory infringements and the fight against corruption*, the subjects within the scope of application of this regulation shall provide information on the Internal Information System on their website.

Likewise, informants will be informed of the existence of external information channels, specifically before the Independent Authority for the Protection of Informants or before the competent authorities at regional, national and European level.

The informant or whistleblower undertakes to make good use of the Internal Information System, refraining from making bad faith, false or misrepresentative reports, with intent to harm, as well as to provide all evidence or clues that he/she may have at his/her disposal, in order to actively collaborate in the clarification of the facts.

6.2.2. Types of communications

6.2.2.1 Ordinary

In order for the complaint to be investigated at the request of a party, with a greater likelihood of investigation and with the guarantee of compliance with all the principles and requirements set forth in this Policy and in the applicable regulations, the communication must contain the following information:

-Relationship with the organization (employee, collaborator, supplier, etc.).
Name and surname, e-mail, address and/or telephone number of the informant.
-The event giving rise to the communication or complaint, as detailed as possible.
-Identification of the natural and/or legal person alleged to have infringed and of any witnesses, in the event that their identity is known.
-Date of the reported events and place or work center affected.
-Evidentiary evidence, if any.

6.2.2.2 Anonymous

Anonymous communications will also be accepted in the Internal Information System, although it is recommended that the informant be identified. In case of an anonymous communication, it must contain the following information, unless it could lead to the identification of the informant:

-Relationship with the organization (employee, collaborator, supplier, etc.).
-The event giving rise to the communication or complaint, as detailed as possible.
-Identification of the natural and/or legal person alleged to have infringed and of any witnesses, in the event that their identity is known.
-Date of the reported events and place or work center affected.
-Evidentiary evidence, if any.

To ensure an effective ex officio investigation and avoid false or misrepresented communications, it is essential to provide sufficient data to initiate the investigation and/or some evidence to support the information, otherwise the anonymous complaint that does not contain this information may be admitted and filed by the System Manager, unless he/she deems it necessary to carry out preliminary investigations based on the credibility of the facts reported.

In both cases, communications must be precise, without omitting any circumstance, avoiding value judgments, and must be aseptic and respectful.

6.3. Acknowledgment of receipt and request for additional information

Upon communication of any irregularity or unlawful behavior through any of WINDAR's internal reporting channels, receipt will be acknowledged.

In communications made through the preferential Online Complaints Channel, the acknowledgement of receipt will be generated automatically and a reference number will be provided, which the informant must note down in order to consult the status of the complaint at any time, whether the communication is anonymous or identified.

For communications received by any other means among those contemplated in this Policy, receipt must be acknowledged within seven (7) calendar days from receipt of the information. In these cases, no acknowledgement of receipt shall be issued when the information provided has been submitted by an anonymous person, or if the informant has been identified, such receipt would jeopardize the confidentiality of the communication.

In the event that the System Manager considers that the information received on the alleged facts is insufficient in any respect, the informant may be asked to expand the information for a maximum period of fifteen (15) calendar days, maintaining anonymity through the online channel or via e-mail, telephone conversation or personal interview in the case of ordinary communications.

6.4. Formation of the dossier and preliminary analysis

For each communication received, an individualized file shall be formed, unless the complaints are made about the same fact or related facts, for which purpose they may be accumulated in the same file.

Prior to the start of the investigation, the System Manager shall conduct a preliminary analysis of the content of the communication, in order to adopt, in a reasoned report, one of the following decisions:

1) Inadmissibility of the complaint when the facts reported are not considered an irregularity or unlawful behavior (see section 4 of this document).

2) Admission for processing and filing of the complaint when the information provided is insufficient to proceed with an investigation, when communication with the complainant to request additional information (necessary to discern the feasibility of the investigation) is impossible, when the facts reported are implausible or when it is about a previous communication without providing new or significant information.

3) Admission of the complaint and initiation of an investigation file, designating the investigating body.

In this phase of analysis of the communication, the System Manager will proceed to inform the complainant of the rejection of the complaint, the filing of the file or the initiation of an investigation procedure, respectively, within a period not exceeding fifteen (15) calendar days from receipt of the complaint or from the end of the period for requesting additional information, if applicable, on an individual basis (when identified) or through the complaint tracking system (in the case of anonymous communications).

6.5. Research

6.5.1. Research planning

The investigation or investigation phase is conceived as a process aimed at clarifying the reported facts, gathering the information necessary for their appropriate resolution.

The person in charge of the Internal Information System shall call, if necessary, a meeting for the constitution of the investigation body, attaching a copy of this Policy and informing the designated members that they must maintain absolute confidentiality and secrecy of any information they may become aware of during the course of the investigation, and must state any incompatibility or circumstance that could affect the objectivity of their decisions.

In the development of the investigation, the System Manager or the investigative body, as the case may be, may require the advice or consultation of other departments of the organization, provided that it contributes to the better clarification of the facts.

The planning of the investigation, always aimed at minimizing the corporate and personal impact on the informant and the subjects under investigation, may contain the following elements:

- Determine the regulations affected and the risks that may arise from the reported facts (economic, legal and/or reputational).
- Identify all documentation whose consultation may be relevant to the clarification of the facts (labor information, e-mails, video surveillance cameras, access records, accounting information, etc.).
- Where appropriate, propose the adoption of precautionary measures with respect to the parties involved in the investigation, in accordance with the provisions of the applicable labor regulations.

6.5.2. Information to the investigated subjects

The person in charge of the Internal Information System shall inform the people reported and any other people who may also be implicated as a result of the investigation carried out, of the facts attributed to them and the identification of the investigating body, as soon as possible and in any case within one (1) month from the date on which the complaint is admitted for processing.

If the System Manager or the investigating body, as the case may be, considers that once informed, the reported person may eliminate any indications or evidence that could compromise him/her, he/she may, in a reasoned and exceptional manner, communicate such data within a period not exceeding three (3) months from the receipt of the communication. This duty of information to the denounced party shall not imply revealing the identity of the denouncer or of third parties involved in the alleged facts.

You will also be informed of your rights regarding the research process and the privacy of your personal data:

- *Personal data protection rights*: the alleged offender must be informed of his rights regarding the processing of his personal data, with the exception that his personal data may not be cancelled during the processing of the complaint file and he may not oppose the processing of his data in the Internal Information System if there are compelling legitimate reasons that justify the need for the processing.
- *Right to a process without undue delay*: the investigation of communications received through the Internal Information System shall be carried out under normal conditions within the time required for their correct resolution, ensuring that the interests of the parties may receive prompt satisfaction.
- *Right to be presumed innocent and not to plead guilty*.
- *Right to reply*: the accused has the right to be heard and to provide as much information as he/she deems appropriate to defend his/her claims.
- *Right not to be penalized for unproven facts*: the accused has the right that in the reasoned report that ends the procedure, only proven facts that have been verified in the investigation carried out are imputed to him/her.

6.6. Research development and documentation

The person in charge of the System or the investigative body, as the case may be, shall ensure the speed of the investigation process, carrying out all the proceedings as soon as possible and always within a maximum period of one (1) month from the moment of its establishment. Said term may be extended in those cases in which the investigated facts are complex, require special technical knowledge or complaints are accumulated, provided that the total term from the receipt of the communication does not exceed three (3) months or, if no acknowledgement of receipt was sent to the informant, within three (3) months from seven (7) days after the communication was made.

In addition, in those cases of special complexity that require an extension of the term, this may be extended up to a maximum of three (3) additional months.

The investigation shall include all the necessary steps for the correct clarification of the facts denounced and of the responsible parties:

i. Appearance of the informant, in the event that he/she is identified. If the informant is anonymous, the communication shall be maintained in such a way as to guarantee his/her anonymity. After the interview, the informant may be granted three (3) working days to provide evidence or request evidence from the investigating body.
ii. Statement of the parties under investigation. The investigating body may grant the accused three (3) working days to provide evidence or request evidentiary proceedings.
iii. Hearing of witnesses or any other people deemed appropriate by the investigative body.
iv. Consultation and analysis of documentation and other evidence collected.
v. Any other proceedings that may be deemed necessary for the clarification of the facts.

All the documents and evidence that have been collected must be included in the complaint processing file, as well as the minutes of the interviews or hearings held (which shall reflect the relevant facts discussed, and must be signed by the Head of the System or the investigating body, as the case may be, and ratified by the rest of the participants).

6.7. Report of findings

The investigating body will prepare a report of conclusions on the following points:

1. *Nature of the facts*: identify, as far as possible, the nature of the facts, date and place of occurrence, people involved and the legal provisions or internal regulations affected.

2. *List of the proceedings and evidence*: the facts gathered in the investigation procedure and the means by which they were obtained shall be described.

3. *Assessment of the facts*: the conclusions will be detailed based on the proven facts, proposing to the Head of the System, as the case may be, (i) the closing of the proceeding because it is not considered to constitute an irregularity or unlawful conduct, the person responsible has not been accredited or the perpetration of the irregular conduct has not been sufficiently justified, or (ii) the continuation of the proceeding if from the proceedings carried out it is considered that the commission of an irregularity or unlawful conduct has been accredited.

4. *Action plan and/or proposed sanction*: in the event that the continuation of the procedure is concluded, a final section should be included identifying the remedial, corrective or improvement measures to be adopted and, if applicable, the sanctions on the responsible party.

This report of conclusions should be filed together with the rest of the investigation file.

6.8. Resolution

6.8.1. Resolution

In the event that an investigation body other than the Head of the System is appointed, it shall decide, within the following seven (7) calendar days, whether it is necessary to carry out additional investigations or whether the investigation has been completed, resuming the investigation or resolving, respectively.

The report issued by the investigating body may be expanded by the System Manager with his assessment of the facts, in the event that it does not coincide in whole or in part with that made by the investigating body, and shall include, as the case may be, those other actions whose adoption could mitigate future non-compliances of the same or similar nature.

The System Manager shall communicate the resolution of the investigation to the management or governing body of WINDAR, providing it with the conclusions report, so that the latter may decide whether or not to adopt the proposed measures or actions and, if appropriate, immediately forward it to the Public Prosecutor's Office if it is determined that the facts constitute a crime, or, where appropriate, to the European Public Prosecutor's Office if the facts affect the financial interests of the European Union.

6.8.2. Sanctions and additional actions

Disciplinary sanctions shall be imposed in accordance with the provisions of the applicable labor regulations (Collective Bargaining Agreement or Workers' Statute), and may be graduated according to the seriousness of the acts committed and the damage caused, and may also take into consideration the recidivism of the offender, the circumstances of vulnerability of the victims, etc. WINDAR's Human Resources Manager will be the executing body of these sanctions.

In those cases in which the assessment of the facts leads to the conclusion of a breach by a supplier, partner or other third party in a business relationship with WINDAR, liability or contract termination actions may be triggered as agreed in each case.

The System Manager will monitor the actions and additional measures, if adopted, following up on the degree of their implementation.

6.8.3. Communication of the resolution

Once the resolution has been adopted by WINDAR's management body, it shall be communicated to the informant and to the person reported.

When the complaint does not result in the imposition of sanctions, because the facts are not considered proven or do not constitute an infringement, the communication of the resolution will correspond to the System Manager, both the complainant and the person reported. When disciplinary sanctions are derived from the complaint filed, the transfer of the resolution to the offenders and its execution will be the responsibility of the Head of Human Resources of WINDAR.

The anonymous whistleblower will be informed of the completion of the investigation procedure through the internal online whistleblower channel, in the section to consult the follow-up status of the communication.

6.9. Preservation of documentation

The personal data declared in the communication shall be kept in the Internal Information System for the time necessary to decide on the investigation of the facts reported, which may not exceed three (3) months from receipt (or six (6) months in cases of particular complexity), unless the purpose of conservation is to leave evidence of the functioning of the Internal Information System. WINDAR shall be subject to the following deadlines regarding the storage of personal data resulting from the receipt of a complaint:

Time of the complaint		Time period for the conservation of personal data
Inadmissibility or filing of the complaint		Information containing personal data may only be provided in anonymized form and must be deleted if this is not the case.
During the investigation of the complaint		Information containing personal data may be stored for the duration of the time that the instruction lasts.
Complaint investigation completed	***Facts not tested***	They should be eliminated unless the purpose of the conservation is to leave evidence of the functioning of the Internal Information System.
	Proven facts	They shall be kept for the duration of the proceedings resulting from the resolution of the investigation (disciplinary and/or judicial) or for the time during which the organization may be held liable. Once completed, they should be deleted unless the purpose of the retention is to leave evidence of the functioning of the Internal System. of Information.

The personal data kept for the purpose of leaving evidence of the operation of the Internal Information System shall be blocked and in no case may the data be kept in the register-book of the communications received and the processing thereof for a period exceeding ten (10) years, proceeding to its deletion after this period (deleting the file and all documentation related to the facts investigated, unless they are kept in an anonymized form).

7. WHISTLEBLOWER PROTECTION

WINDAR recognizes and facilitates, in addition to enabling an Internal Reporting System to prevent and detect irregularities or illegal behavior, access to a series of protection and support measures for whistleblowers.

The use of the Internal Information System by all those subjects contemplated as possible informants (see section 4 of this policy) is governed by the following principle

The Company is committed to maintaining the confidentiality of the identified whistleblower, although, in accordance with current legislation and in order to enhance the confidentiality of the whistleblower, the possibility of reporting any communication anonymously is recognized.

Despite this, there is no zero risk of identification of the anonymous whistleblower during the investigation, so it is important to establish procedures to protect against possible retaliation for reporting any irregularities or illegal behavior.

The recognition of measures to prohibit retaliation within the organization is at the heart of WINDAR's efforts to protect and defend the integrity of whistleblowers who report wrongdoing or unlawful behavior in the context of an employment or professional relationship with the organization.

The prohibited actions to avoid incurring in acts constituting retaliation and the conditions required for the whistleblower to be covered by the protection and support measures regulated in articles 37 and 38 of *Law 2/2023, of February 20, regulating the protection of people who report regulatory infringements and the fight against corruption,* are set forth below.

7.1. Scope of protection

Informants, whether identified or anonymous and subsequently identifiable, will need to meet the following requirements in order to be eligible for protection measures after making communications through WINDAR's Internal Reporting System:

a) That the informant has well-founded reasons that prove the truthfulness of the communication.
b) That the informant reports violations within the scope of application of *Law 2/2023, of February 20, regulating the protection of people who report regulatory violations and the fight against corruption*.
c) That the whistleblower has used any of the internal reporting channels provided by WINDAR to communicate the information or has reported directly to the competent authorities.

However, whistleblowers who, notwithstanding the foregoing, submit communications that have been previously rejected by the Internal Reporting System or the Independent Whistleblower Protection Authority, are related to interpersonal conflicts or only affect the whistleblower and the accused in their private sphere, are public, constitute mere unsubstantiated rumors, or are not covered by this Policy, shall not be entitled to protection.

7.2. Prohibition of retaliation

WINDAR undertakes to avoid any type of act that may constitute retaliation, including, in general, threatening attitudes or attitudes that may be considered as attempts at retaliation in accordance with the provisions of Article 36 of *Law 2/2023 of February 20, regulating the protection of people who report regulatory violations and anti-corruption*.

In any case, retaliation shall be considered any act or omission prohibited by law, or that, directly or indirectly, entails unfavorable treatment that places the people who suffer it at a particular disadvantage with respect to another in the labor or professional context, solely because of their status as whistleblowers.

8. VALIDITY AND REVISION

This Policy for the management of the Internal Information System and whistleblower protection shall enter into force on the date of its approval by the WINDAR management body, and shall remain in force until the aforementioned body approves its update, revision or repeal, after consultation with the legal representatives of the employees.

The compliance and effectiveness of this Policy will be reviewed annually, and modifications and updates that contribute to its development and continuous improvement will be proposed to the Board of Directors, if necessary.