Internal Information System Policy

1. Introduction and Purpose

This Policy is intended to promote and enhance the culture of communication within the organization, as a tool to prevent and detect threats to the public interest. It will also ensure and prioritize the protection of whistleblowers and individuals making reports, under Law 2/2023 of February 20th, regulating the protection of persons who report regulatory violations and the fight against corruption, implementing DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of October 23rd, 2019, on the protection of persons who report breaches of European Union law, in Spain.

Maths for More, S.L. (hereinafter, Wiris) expects both its members and its business partners to consistently act in accordance with the principle of good faith when performing their duties. Among other things, this requires maintaining an unwaveringly collaborative attitude towards the organization.

As a tool for compliance with the above, Wiris has set up the following internal whistleblower channel. This acts as a first-line channel available to all managers, employees, collaborators, and suppliers of the organization, as well as any other third party. It can be used by accessing the following form: whistleblowersoftware.com/secure/wiris or by sending a written communication by mail to C/ de Roger de Flor, 221, Bajos, 08025 Barcelona, Attn: Party Responsible for the Internal Information System, or in a face-to-face meeting, sending the meeting request through any of the above means of communication.

2. Scope

This Internal Information System Policy applies to and is binding for all members of Wiris.

This Policy is translated into every language necessary so that all Wiris members and the third parties associated with the organization can understand its scope and content.

3. Content of Communications

Through this Internal Information System, managers, employees, collaborators, suppliers, and other third parties can confidentially and anonymously report any concern regarding a possible non-compliance or violation of the provisions of the Code of Conduct or any other internal Policy of the organization. They can also report a violation or omission they are aware of that may constitute an infringement of European Union law or contravene its financial interests, including criminal and/or administrative breaches of Spanish law.

In this regard, this internal channel may be used to report actions or omissions that constitute or may constitute violations in the following areas:

- Harassment/discrimination

- Public procurement
- Confidentiality
- Corruption/fraud
- Competition
- Corporate crimes
- Tax/corporate matters
- Non-compliance with current legislation
- Non-compliance with internal policies, procedures and regulations
- Non-compliance with the Code of Conduct and other internal codes
- Labor/workers' rights
- Environment
- Intellectual property/trade secrets
- Organizational protocols and standards
- Occupational risk prevention
- Consumer protection
- Protection of privacy and personal data
- Risk of or suspected money laundering or financing of terrorism
- Sustainability
- Public health
- Security of networks and information systems
- Product safety and compliance
- Transportation safety
- Other

This whistleblower channel shall only be used for the purpose described and shall not be used as a conduit for organizational complaints.

The internal information channels that are set up to receive any communications or information other than that established above are not covered by this Policy or by Law 2/2023 of February 20th, which regulates the protection of persons who report regulatory violations and the fight against corruption.

4. Whistleblowers or Informants

The principles, guarantees, and rights set forth in this Policy are focused on protecting whistleblowers or informants, prohibiting retaliation in any form and encouraging support and assistance for these individuals.

In this context, whistleblowers or informants are considered any natural person that reports the infractions mentioned above, that works in the private or public sector, and has obtained information on infractions in a workplace or professional context, including in all cases:

Employees, including those whose work or professional relationship with the company has already ended.

- Self-employed individuals.
- Volunteers.
- Interns.
- Individuals going through the hiring process.
- Partners, shareholders.
- Members of the administrative board.
- Anyone working under the supervision of contractors, subcontractors, or suppliers.

Additionally, in compliance with the above-mentioned Law 2/2023, the following will also be protected by this Policy:

- the legal representatives of workers, in the exercise of their functions of providing advice and support for the whistleblower.
- natural persons who, within the framework of the organization in which they provide services to the whistleblower, help the latter during the process.
- natural persons who are related to the whistleblower and who may experience retaliation, such as coworkers or family members of the whistleblower.
- legal entities for whom they work or with whom they maintain any other kind of relationship in a work context or in whom they have a significant stake. In this sense, a significant stake is understood to be when the share capital or voting rights corresponding to shares or equity allows the person possessing them to have an influence on the legal entity in question due to the proportion of those shares or equity owned.

5. General Principles and Guarantees

5.1. Integration of Internal Channels

The whistleblower channel that comprises Wiris' Internal Information System shall be available and accessible to all workers and any third party, regardless of their relationship with the organization. It is a comprehensive and first-line channel to report on the actions or omissions set forth in section 3 of this Policy.

5.2. Confidentiality and Anonymity

Wiris guarantees both the confidentiality and anonymity of the whistleblower and of any third party that is or may be mentioned and/or involved in the communication, in the actions carried out in connection therewith, or in its processing. It is not necessary to obtain information that will allow for their identification. Accordingly, the protection of the data is guaranteed, and unauthorized personnel are prevented from accessing it.

Thus, the proceedings that are carried out with regard to third parties or other entities, areas, or departments of the organization must be completed while maintaining the anonymity of the WHISTLEBLOWER and the PARTY UNDER INVESTIGATION, also keeping the reasons for the communication as secret as possible.

Wiris guarantees that the identity of the whistleblower can only be revealed to the judicial authority, prosecuting authority, or competent administrative authority as part of a criminal, disciplinary, or sanctioning investigation.

All those who for various reasons may participate in supporting roles during the investigation of a specific incident should sign the pertinent Confidentiality Agreement.

In those cases where the receiving of communications is managed by an external supplier, it shall always be verified that said supplier offers sufficient guarantees to respect the independence, confidentiality, data protection, and secrecy of the communications.

In cases where the communications are sent via internal channels that are not those established by Wiris, or communications are sent to staff members who are not responsible for their processing, the organization guarantees the preservation of confidentiality as described above. To this end, there is a Plan for Regular Compliance Training, in which it will be advised (following the requirement set forth in art.9.2.g of Law 2/2023) that non-compliance implies a very serious infraction of the Law and that, in addition, the person receiving the communication should immediately send it to the Party Responsible for the System.

5.3. Presumption of Innocence and Honor

Wiris shall, at all times, guarantee the presumption of innocence and honor of all persons affected by a communication.

The persons affected by a communication shall have the right to be informed of the actions or omissions they are accused of, as well as to be heard over the course of the investigation. In no case will the identity of the whistleblower be revealed to them.

Wiris guarantees the following to the persons affected by the communication: the right to the presumption of innocence, the right to defense and the right to access the file as set forth in Law 2/2023, as well as the same protection established for whistleblowers, preserving their identity and guaranteeing the confidentiality of the facts or events and information on the proceeding.

5.4. Access to External Channels and Public Disclosure

The whistleblowers or informants can send their communication through the external channel of the state authorities, the Anti-Fraud Office of Catalonia, or the authorities or corresponding entities in other applicable autonomous communities, whether directly or with the communication being sent first through this internal channel.

In addition, the whistleblowers or informants are made aware of the possibility of public disclosure.

Public disclosure consists of making the information on the facts or events that are detailed in the communication through this Information System available to the public.

In this context, in order to enhance the protection of Law 2/2023, concerning people making public disclosures, the following conditions must be met:

a. The communication must first have been made via internal and external channels, or directly through external channels, without appropriate measures having been taken in this respect within the timeframe established.

b. There must be reasonable reason to think that either a) the infraction may entail an imminent or clear danger to the public interest or there is a risk of irreversible damage, including risk of harm to the physical integrity of a person, or b) in the case of communication through an external information channel, there is a risk of retaliation or there is a low probability that the information will be processed effectively given the particular circumstances of the case, such as the concealment or destruction of evidence, collusion between an authority and the person committing the infraction, or the authority being involved in the infraction.

5.5. Prohibition of Retaliation

Wiris expressly prohibits any acts constituting retaliation, including threats of retaliation or attempts at retaliation, against individuals submitting a communication.

Retaliation is understood as any act or omission that is prohibited by law, or that directly or indirectly entails unfavorable treatment of individuals that puts them at a disadvantage with respect to other people in the work or professional context, based only on their condition as whistleblowers or having made a public disclosure.

For the purposes of that set forth in Law 2/2023 and by way of example, article 36 of said regulation establishes the following list of things that may be considered retaliation:

a) Suspension of the work contract, dismissal, or termination of the work or statutory relationship, including non-renewal or early termination of a temporary work contract once the trial period has passed, or the early termination or cancellation of contracts for goods and/or services, the imposition of any disciplinary measure, demotion, or denial of promotions and any other substantial modification of the work conditions, as well as not changing a temporary work contract to a permanent one, in cases where the worker had legitimate expectations of being offered a permanent position, unless these measures take place within the normal exercise of management powers under the labor laws or legislation regulating the statute of the corresponding public employee, due to demonstrable circumstances, facts, or infractions that have nothing to do with the presentation of the communication.

b) Damages, including those to a person's reputation, economic losses, coercion, intimidation, harassment, and ostracism.

c) Negative evaluations or references in connection with the individual's work or professional performance.

d) Inclusion on blacklists or spreading information in a particular sector that interferes with or hinders the individual's access to employment or ability to be hired for work or services.

e) Denial or cancellation of a license or permit.

f) Being denied training.

g) Discrimination, or unfavorable or unfair treatment.

Once a period of two years has elapsed, the individual whose rights were violated in connection with their communication or disclosure may request protection from the competent authority, who, exceptionally and with due justification, can extend the protection period following a hearing with the people or entities that may be affected. Being denied an extension of the period of protection should be justified.

5.6. Support Measures

In accordance with the rules established by Law 2/2023, the organization makes available to the whistleblower or informant the ideal means of support required, following the evaluation of the circumstances.

All of this is notwithstanding the assistance they may be entitled to under Law 1/1996 of January 10th, on free legal assistance, for representation and defense in legal proceedings stemming from submitting the communication or carrying out the public disclosure.

5.7. Measures of Protection against Retaliation: exemption from liability

Individuals who notify or reveal infractions, as defined in section 3 of this document, will have the right to protection as long as the following circumstances are met:

a) they have reasonable grounds to think that the information in question is true at the moment of the communication or disclosure, even when they do not provide conclusive evidence, and the information is covered by the scope of Law 2/2023.

b) the communication or disclosure was made in accordance with the requirements set forth in Law 2/2023.

People who communicate or disclose the following are expressly excluded from the protection envisaged in this law:

a) Information contained in communications that were rejected by any internal information channel or for any of the reasons set forth in article 18.2.a) of Law 2/2023.

b) Information associated with complaints regarding interpersonal conflicts or that affect only the whistleblower or the people to whom the communication or disclosure refer.

c) Information that is already fully available to the public or that is just circulating in the form of rumors.

d) Information that refers to actions or omissions that are not included in section 3 of this document.

Individuals who have communicated information in accordance with this Policy will not be considered to have violated any restriction on revealing information, and will not be held liable in connection with said disclosure, as long as they had reasonable grounds to believe that this communication or public disclosure was necessary to expose an action or omission pursuant to this Policy.

Whistleblowers shall not be held liable with respect to the acquisition of or access to information that is communicated or publicly disclosed, as long as said acquisition or access does not constitute a crime.

5.8. Personal Data Protection

Wiris is committed to processing data contained in communications in strict compliance with the legislation on personal data protection and whistleblowers, ensuring there is no retaliation at any time.

The processing of personal data under Law 2/2023, on which this Policy is based, is governed by the provisions of Section VI of said Law, those of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016, those of Organic Law 3/2018 of December 5th, on the Protection of Personal Data and the guarantee of digital rights, and those of Organic Law 7/2021 of May 26th, on the protection of personal data processed for the purposes of the prevention, detection, investigation, and judgment of criminal offenses and the enforcement of criminal penalties.

Personal data that is not clearly required to process specific information shall not be collected. If it is accidentally collected, it shall be deleted without undue delay.

6. Commitment to Compliance

Everyone connected with Wiris in any way should be familiar with the ethical principles and principles of responsibility, as well as all of the provisions and obligations contained in the different control measures adopted by the organization. Compliance with these is obligatory and these parties must undertake to preserve the integrity and reputation of the company.

This Policy, along with the Code of Conduct and the other Protocols, Policies, and Internal Regulations implemented by Wiris are a fundamental pillar of the organization's culture of compliance. For this reason, this Policy is compulsory for everyone linked to the organization, as well as for all business partners. They are thus required to comply not only with the current legislation, but also to show loyalty to the values and ethical principles and principles of responsibility of the organization.

To facilitate knowledge of this Policy, as well as its compliance, it is made available to all of the members of the organization and to the interested third parties.

7. Penalty System

Any action that may entail a limitation of the rights and guarantees for whistleblowers, of their confidentiality and anonymity, or non-compliance with the secrecy of the information received and the data contained therein, may constitute a serious or very serious infraction

of the provisions of Law 2/2023, of February 20th, regulating the protection of persons who report regulatory violations and the fight against corruption.

8. Responsibility and Supervision

Wiris' Compliance Committee is the collective body responsible for this Internal Information System and is in charge of ensuring its correct operation. It will also make sure that the information received is processed appropriately. In addition, this collective body delegates the ability to manage the system and process the investigation files to one (1) of its members (Annex 1 of this document).

The Compliance Committee independently and autonomously carries out its functions, and it was duly designated by the governing body of Maths for More, S.L., with this designation being communicated to the competent authority in the manner and within the timeframe established by law.

This Policy shall be reviewed and/or modified by the Party Responsible for the Internal Information System, who may outsource the service to specialists:

1. Whenever there are important changes in the organization, in the control structure, or in the activity carried out by the entity that make this advisable.
2. Whenever there are legal changes that make this advisable.
3. Whenever important violations of its provisions occur that make this advisable.

This Policy will be reviewed periodically, even when none of the circumstances described above have occurred.

9. Approval

This Internal Information System Policy has been approved by the governing body of Maths for More, S.L. and may be modified to improve the confidentiality and effectiveness of the management of the communications received.

10. Documents related to this Policy

- Communications Management Procedure.
- Code of Conduct.

11. Annexes

Annex 1) Compliance Committee and Party Responsible for the System:

Members of the Compliance Committee and the delegated person responsible for the internal information system
Position
Carolina Brizzio - Party Responsible for the Internal Information System
Gaspar Pérez
Aida González

12. Version History

Version	Date	Approved by	Reason for change
Original V.	29/11/2023	Compliance Committee	