Suma Capital
GROWING TOGETHER

SUMA CAPITAL, S.G.E.I.C, S.A., Sociedad Unipersonal

INTERNAL INFORMATION SYSTEM PROTOCOL

Version	Date	Affects	Brief description of the change
1	**22 May 2020**	**Creation**	
2nd	**15 May 2023**	**Update**	**Adaptation to Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, transposing Directive (EU) 2019/1937 of the European Parliament.**
3rd	**24 May 2024**	**Update**	**Incorporation of Net Zero Ventures, S.L.**
4th	**11-11-2024**	**Update**	**Inclusion of clarifications regarding the definition of infringements and data protection, and express inclusion of external information channels**

TABLE OF CONTENTS

1. INTRODUCTION

In accordance with the requirements set forth in Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, transposing Directive (EU) 2019/1937 of the European Parliament (hereinafter "Law 2/2023") and Article 31bis of the Criminal Code, **SUMA CAPITAL, S.G.E.I.C, S.A., Sociedad Unipersonal, and Net Zero Ventures, S.L. (**hereinafter "NZV"), an advisory company for some of the funds managed by SUMA CAPITAL S.G.E.I.C., S.A., Sociedad Unipersonal (hereinafter jointly referred to as **"SUMA CAPITAL"**) have proceeded to create an Internal Reporting System.

Law 2/2023 establishes in Article 10 that private sector companies with 50 or more employees are required to have an Internal Information System, as are those that, despite not meeting this threshold, have implemented an Internal Information System. Likewise, the Criminal Code, within the framework of the implementation of the Crime Prevention Model, in Article 31.bis.5. 4º, requires companies to report risks and breaches of the Crime Prevention Model (hereinafter "CPM") to Compliance Officers.

Therefore, and given that the entity's main interest is the creation of a corporate culture of legal compliance, the Internal Information System has been created and this Protocol has been developed.

2. IDENTIFICATION

2.1. PURPOSE

The purpose of this document is to establish the procedure for processing reports of infringements received through the Internal Reporting System, including the guidelines to be followed from the moment the report of infringement is received by the Compliance Officer or the External Manager until a resolution is reached, following processing and investigation.

The Internal Information System is one of the key controls established in the MPD for the prevention, detection and reporting of ethical breaches, regulatory non-compliance or criminal offences, meaning that the guidelines set out in this Protocol are mandatory for all persons associated with the entity.

The entity shall provide the Compliance Officer with all the necessary resources NZV to properly process and resolve reports of violations received through the Internal Information System, also granting them sufficient authority, autonomy and access to the entity's information to perform their duties.

2.2. SCOPE OF APPLICATION

This Protocol is applicable and mandatory for all members of the organisation. The term "member" includes:

- Employees of the entity.
- Shareholders, participants or persons belonging to the Administrative Body.
- Professionals and collaborators linked to the entity over whom it may exercise direct or indirect control.
- Interns.

3. DEFINITIONS

3.1. **Internal Information System:** Channel established by the entity for reporting infringements within its scope.

3.2. **External Information Channel of the Independent Whistleblower Protection Authority:** Information system managed by a state authority, as well as regional authorities, which employees of the entity can use.

3.3. **Breaches:**

- Breach of internal regulations.
- Any actions or omissions that may constitute infringements of European Union law, provided that:
    - They fall within the scope of the European Union acts listed in the annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, regardless of how they are classified under domestic law;
    - Affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or
    - Have an impact on the internal market, as referred to in Article 26(2) TFEU, including infringements of European Union rules on competition and State aid, as well as infringements relating to the internal market in connection with acts that infringe
      corporate tax rules or practices whose

purpose is to obtain a tax advantage that distorts the object or purpose of the legislation applicable to corporate tax.

- Actions or omissions that may constitute a serious or very serious criminal or administrative offence. In any case, this shall include all serious or very serious criminal or administrative offences that involve financial loss to the Treasury and Social Security.

3.4. **Whistleblower: A** person who reports an offence.

3.5. **Person under investigation:** Person against whom the offence report is filed and who, as a result of the investigation, may be subject to disciplinary action or may be held criminally or administratively liable.

3.6. **Affected person:** Person who suffers the actions of the person under investigation other than the Whistleblower (if applicable).

3.7. **System Manager:** Person responsible for the Internal Information System appointed by the Management Body and in charge of managing and processing investigation files. In this case, the System Manager will be the entity's Compliance Officer.

3.8. Person **responsible for the investigation:** person appointed by the Compliance Committee to carry out the investigation of a report of an infringement.

3.9. **External Manager:** External lawyers who manage the Internal Reporting System.

3.10. **Independent Whistleblower Protection Authority (A.A.I):** State and regional authorities responsible for managing the external reporting system and processing complaints filed through that system.

4. INTERNAL REPORTING SYSTEM

4.1. REPORTING A VIOLATION

Violations may be reported in writing or verbally. Regardless of the means of communication used, in the event that a conflict of interest may arise in the handling of such reports, or if external management is considered preferable for any reason, they will be handled by the External System Manager, ASESORIA PENAL CORPORATIVA (hereinafter, "APC").

4.1.1. Reporting violations in writing:

4.1.1.1. Online platform: An internal information system has been set up on the FACTORIAL platform, which can be accessed by all employees of SUMA CAPITAL, S.G.E.I.C., S.A, Sociedad Unipersonal, for the secure and confidential reporting of infringements, and which will be the preferred channel for reporting. NZV employees will have access to this communication channel via the following link, which is also available on the website of SUMA CAPITAL, S.G.E.I.C., S.A, Sociedad Unipersonal: Suma Capital - Secure channel

Through the platform, members of the organisation can access a form through which they can submit nominative or anonymous information. This information will be managed by the Head of the Internal Information System.

After submitting the report, the informant may access the platform at any time to check the status of the infringement report.

4.1.1.2. Email: alternatively, the whistleblower may send an email to the Compliance Officer, Head of the System

Internal Reporting System: Ms GRISELDA GARDE (ggarde@sumacapital.com) or the External Manager APC (proyectos@asesoriapenalcorporativa.es) to report a violation.

4.1.1.3 Postal mail: alternatively, the whistleblower may submit the information in writing by post to the Compliance Officer at the entity's registered office[1].

4.1.2. Verbal reporting of violations:

4.1.2.1. In person: at the request of the whistleblower (in the details indicated above), the information may be presented in person or online with the Compliance Officer and/or the External Manager within seven days of the request. The information provided during the face-to-face or remote meeting must be recorded. In this regard, the Compliance Officer and/or External Manager must inform the whistleblower of this fact and explain how their data will be processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

4.1.2.3 Information communicated by other means: in the event that information is sent by other means or channels not established in this protocol, or to members of the organisation who are not responsible

1Av. Diagonal, nº. 640, (08017), Barcelona. CIF: A64096563

of its processing, it must be communicated by the recipient through the organisation's internal information system.

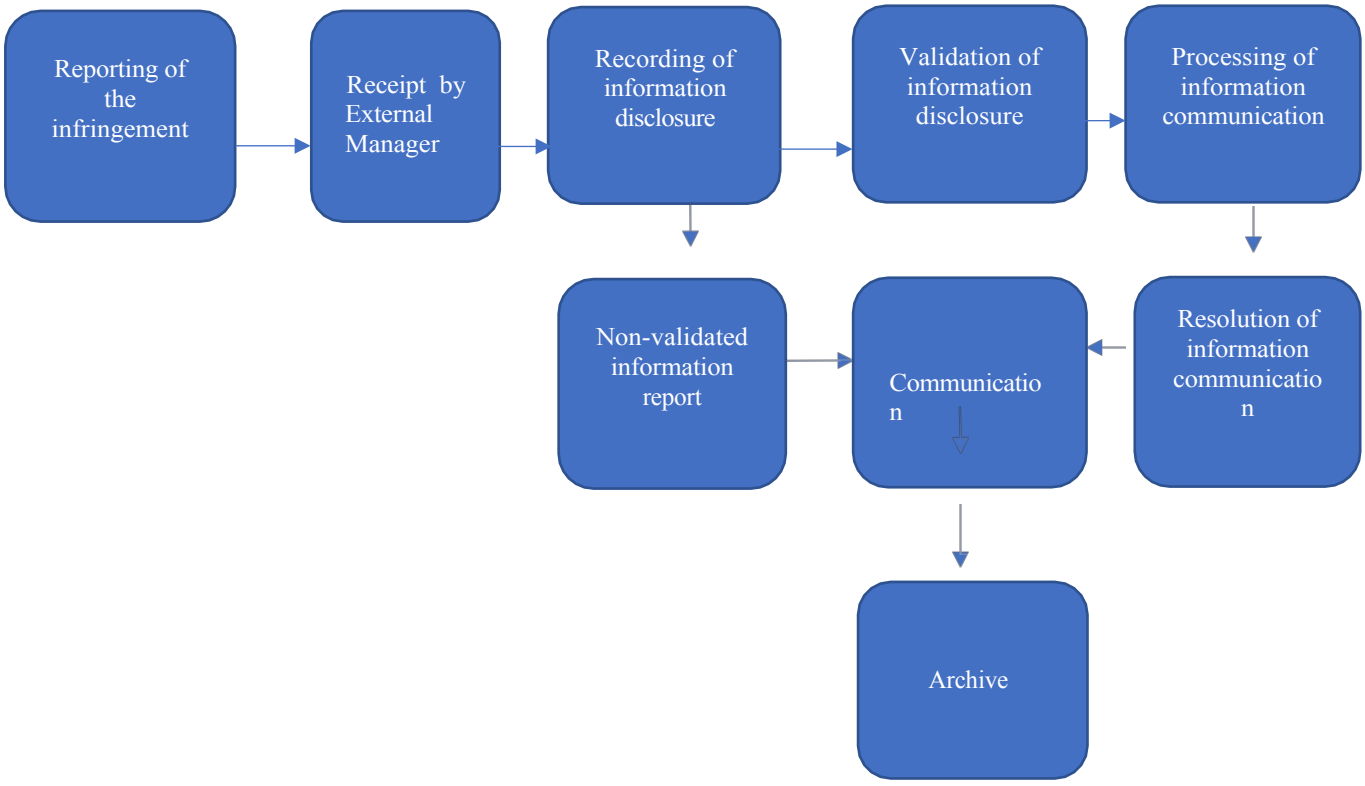
4.2. CONTENT OF THE REPORT OF THE INFRINGEMENT

The content of the breach report must be as follows:

- Identification of the informant (full name, national identity number, email address and relationship with the entity) or select the anonymous option.
- Identification of the department and/or activity where the events took place or where the evidence referred to became known.
- Name of the person(s) under investigation or delimitation of the area (if known).
- Description of the events and circumstances in which they occurred.
- All evidence available to the informant that is relevant, appropriate and lawful.
- Date on which the events took place.
- Persons who witnessed or have knowledge of the events.
- How the reported event came to light.

All communications of information must be made in good faith.

4.3. PROCEDURE



4.3.1. **Receipt of the report of infringement**: APC, as External Manager, and the Compliance Officer, as Head of the Internal Information System, will receive the report of infringement through the platform or the alternative means referred to above, and the actions taken will be recorded.

The Compliance Officer or, if necessary, APC will have seven calendar days from receipt to send an acknowledgement of receipt to the whistleblower, unless this could jeopardise the confidentiality of the report.

4.3.2. **Recording of the report of infringement:** Once the report has been submitted via the platform, it will be recorded.

automatically on the platform. If the information is submitted by other means, such as a face-to-face meeting, the relevant information must be recorded by the Compliance Officer and/or the External Manager.

4.3.3. **Valid reporting of violations:** If the report of the violation refers to breaches that fall within the scope of the Channel (violations indicated in point 3.3), the report of the violation will be validated.

4.3.4. **Communication of invalid information:** in the event that the communication of information refers to facts that

- fall outside the objective scope of application of the channel (point 3.3.) or are manifestly unfounded: this will be communicated to the whistleblower and the communication of information will be archived,
- are outside the scope of the channel but relevant to the entity: they will be forwarded to the relevant department for handling the incident, the informant will be notified, and the communication of information will be archived.

4.3.5. **Processing of the breach report:** breach reports that have been previously validated will be processed. This means that the relevant internal investigation will be initiated. In this regard, the Compliance Officer, as the person responsible for the Internal Information System, will appoint an Investigation Manager if deemed necessary. If the information has been handled by the External Manager, it will be shared with the Compliance Committee, in accordance with the conflict of interest rules set out in section 5.3 of this protocol. Where appropriate, the recipient of the information may appoint an Investigation Manager.

In this regard, the internal investigation may be carried out by:

- one or more members of the Compliance Committee who are not affected by the information.
- a member of the entity deemed competent if the information directly affects all members of the Compliance Committee.
- an external expert or advisor.
- a body composed of several persons from the entity, with or without an external expert or advisor, provided that there is no incompatibility or conflict of interest with regard to them.

The Head of Investigation shall carry out the actions they deem necessary, either individually or in collaboration with the persons they deem necessary, provided that there is no incompatibility or conflict of interest between them. To this end, they may gather all the information and documentation they deem necessary from any area, division or department, always respecting the fundamental rights of the person(s) under investigation. If deemed necessary, an external expert advisor may be engaged as a necessary and indispensable complement to safeguard the guarantee of independence in the investigation and preparation of the opinion.

In this regard, during the investigation, the person responsible for it may communicate with the informant and, if deemed necessary, request additional information.

The maximum duration of the investigation proceedings shall be three months from the receipt of the report of the infringement until the resolution thereof or, if no acknowledgement of receipt was sent to the informant, from the end of the seven-day period following the report. In particularly complex cases, which must be justified in writing by the person responsible for the investigation, it may be possible to extend the duration of the investigation proceedings.

extend the deadline by an additional three months.

4.3.6. **Resolution of the infringement report:** Once the investigation has been completed, the Head of Investigation will prepare a report to be shared with the Compliance Officer and the members of the Compliance Committee for approval and subsequent reporting to the Administrative Body.

4.3.7. **Communication to the Whistleblower:** Once the report has been approved, the Whistleblower will be informed that the processing of the report has been completed and that it will be archived.

4.3.8. **Archiving**: After notifying the Whistleblower, the report will be archived.

The entire procedure will be reflected on the online platform, which will be accessible to the Whistleblower who has submitted a report so that they can check the status of its processing (not its content). If the report has been submitted by email, telephone or in person, communications will be made by email.

The above will apply except in cases where the Informant indicates that they do not wish to receive information about the procedure, in which case no communication will be sent to them.

Reports made to the Administrative Body shall include information relating to the communication of information processed, omitting any information that could identify the informant, i.e. the information in the report shall be anonymised.

5. EXTERNAL INFORMATION CHANNEL

Any person may report the commission of any action or omission included within the scope of this Protocol to the Independent Whistleblower Protection Authority (A.A.I.) or to the corresponding regional authorities or bodies.

European Union	European Anti-Fraud Office (OLAF) https://anti-fraud.ec.europa.eu/index_en
Catalonia	Anti-Fraud Office of Catalonia https://www.antifrau.cat/es/investigacion/denuncia.html

This communication can be made directly, or after prior communication through the Internal Information System enabled by SUMA CAPITAL.

The authorities designated for the management and processing of communications received through external information channels are detailed below:

6. RIGHTS, PRINCIPLES AND GUARANTEES

6.1. RIGHTS OF THE INFORMANT

The whistleblower shall have the right to:

- Decide whether to make the communication anonymously or not anonymously. In the latter case, the booking of the whistleblower's identity is guaranteed.
- Make the report verbally or in writing.
- Indicate a place where communications can be received: home address, email, telephone, etc.
- Waive their right to receive communications.
- Appear before the Head of the Internal Information System or the Head of the Investigation if they deem it appropriate.

- Request that the appearance be made by videoconference or other telematic means that guarantee the identity of the informant and the security and fidelity of the communication.
- Exercise the rights conferred by legislation on the protection of personal data.
- Report any actions or omissions included within the scope of this protocol and Law 2/2023 through the External Information Channel managed by the Independent Whistleblower Protection Authority, either directly or after reporting them through the organisation's Internal Information System.

6.2. PRINCIPLES AND GUARANTEES

All members of the entity have the right and obligation to report through the Internal Information System.

The availability of access to the Internal Information System by members of the entity as an incentive to comply with their duty to report infringements entails the need to protect the whistleblower.

To this end, the following guarantees shall apply to the management and processing of information:

6.2.1. **Autonomy and Independence of the System Manager:** the System Manager, as well as the other members of the Compliance Committee, are guaranteed their autonomy through formal appointment, and therefore undertake to ensure the confidentiality and protection of the Whistleblower without accepting pressure or interference from members of the Management Body or any other area that may be involved in the receipt of a report of a breach.

6.2.2. **Confidentiality and secrecy of communications**: Confidential treatment that prevents the disclosure of personal data, as well as any details that would allow the Whistleblower to be identified by the persons or departments related to the communication, or by any professional within the entity other than the Compliance Officer or a member of the Compliance Committee. The identity of the Whistleblower may only be disclosed to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

6.2.3. **Prohibition of Retaliation**: The filing of a report made in good faith, regardless of the accuracy of the information in terms of truthfulness, shall not give rise to any retaliation against the Whistleblower in the workplace. Nor shall pressure be exerted, in terms of moral or psychological harassment, with the aim of influencing the cessation of the accusations or as revenge for them.

This is a commitment made, through the approval of this Protocol, by the Compliance Officer, the Compliance Committee and the Administrative Body. This prohibition and the consequent protection of the Whistleblower from possible reprisals shall remain in force for a period of two years after the completion of the internal investigation proceedings.

6.2.4. **Protection of the Whistleblower**: The members of the Compliance Committee and, in particular, the Head of the Internal Information System shall be responsible for ensuring the protection of the Whistleblower, guaranteeing the non-disclosure of their identity and personal data, as well as the absence of negative consequences for reporting information. If the Whistleblower is required to provide additional information or testimony in order to verify the accuracy and seriousness of the report, they shall be entitled to legal representation at their request.

The communication must be carried out in such a way as to ensure that the aforementioned levels of protection are maintained in both the request and the response.

6.2.5. **Absence of conflicts of interest**: No person related to the communication shall be involved in its processing and investigation.

6.2.6. **Absence of conflicts of interest in the decision-making of the Administrative Body:** Members of the Administrative Body who may be affected by the communication of information shall refrain from participating in the decision-making process for the resolution of the communication.

6.3. CONFLICT OF INTEREST

- Reports will be received and processed by the Compliance Officer and the External Manager.

- If the communications involve a conflict of interest affecting the Compliance Officer, they shall be forwarded by the External Manager of the Internal Information System to the Compliance Committee for processing, with the Compliance Officer being excluded from the process.

- If the communication of information affects one or more members of the Compliance Committee, it shall be forwarded to and dealt with by the members of the Committee who are not affected by it.

- If the communication of information affects all members of the Compliance Committee, it shall be forwarded by the External Manager of the Internal Information System to the Board of Directors, which shall manage the investigation and

proposed action.

- In the event that the communication of information affects all members of the Compliance Committee, the Compliance Officer and any member of the Board of Directors, it shall be forwarded by the External Manager to the members of the Board of Directors not affected by the communication of information, and the investigation and proposed action shall be managed with them.

6.4. RIGHTS OF PERSONS UNDER INVESTIGATION

The person under investigation has the right to the presumption of innocence, the right to honour, the right to defence, the right to be informed of the actions or omissions attributed to them, the right to have access to the file during the proceedings and the right to be heard at any time. The communication and information referred to shall take place at the time and in the manner deemed appropriate by the Head of the Investigation to ensure the successful outcome of the investigation.

Likewise, the persons under investigation shall be entitled to the same protection established in this protocol for whistleblowers in relation to the preservation of their identity and the confidentiality of the facts and data of the proceedings.

Access to the file by the person under investigation shall be in relation to the facts under investigation, without access that would allow the identity of the whistleblower and third parties mentioned in the information provided to be identified. Therefore, in each specific case, the person responsible for the investigation shall decide which documents and information may be shared with the person under investigation if requested.

7. REPORT AND REGISTRATION OF THE COMMUNICATION OF INFORMATION PROCESSED

A record of each communication of information is kept in the numbered Internal Information System, which will record the receipt of the communication, the date of filing, the area of the entity affected, the investigation carried out, the actions taken and the corrective measures implemented. Only the Compliance Officer and the External Manager of the Internal Information System will have access to the information indicated.

The information indicated will be stored indefinitely in the system in order to prove the functioning of the system in the event of a possible judicial investigation as a central element of SUMA CAPITAL's Crime Prevention Model.

8. PROCESSING OF PERSONAL DATA

The processing of personal data resulting from the application of this policy shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December on Data Protection and Guarantees of Digital Rights, Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, and TITLE VI of Law 2/2023 of 20 February regulating the protection of persons who report regulatory infringements and the fight against corruption, transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report infringements of Union law.

Data subjects may exercise the rights set forth in Articles 11 to 22 of Regulation (EU) 2016/679. Specifically, data subjects may exercise their (i) right of access, (ii) right to rectification, (iii) right to erasure, (iv) right to object, (v) right to restriction, and (vi) right to data portability by sending a letter marked "Data Protection" and accompanied by a copy of both sides of their national identity card or equivalent document to the Data Controller in person or by email todpo@sumacapital.com .

However, if the person to whom the facts described in the communication refer exercises their right to object, it will be presumed that, unless proven otherwise, there are compelling legitimate grounds that justify the processing of their personal data.

Access to the data contained in the Internal Information System shall be limited to:

- External manager of the Internal Information System, as the party responsible for processing the aforementioned data.
- The entity, as the Data Controller. In this case, the entity will grant access to the data contained in the Internal Information System to the System Manager, the HR Manager when disciplinary measures may be taken against an employee, or the entity's Legal Services Manager if legal measures are to be taken in relation to the facts reported in the communication.
- The Data Protection Officer, where applicable.

The scope of data processing shall be as follows:

- Registration of communications received through the online platform enabled as the Internal Information System.

- Retention of data received. The data will be retained for the period strictly necessary to decide whether to initiate an investigation, which may not exceed three months or, in any case, ten years, in accordance with the provisions of Article 26.2 of Law 2/2023 of 20 February.
- Deletion of data received in the following cases:
    - Three months after receipt of the communication without any investigation having been initiated, unless the purpose of the retention is to leave evidence of the functioning of the system.
    - When the data refers to conduct that does not constitute any type of offence.
    - When the information received contains personal data included in the special categories of data.
    - If it is proven that the information provided, or part of it, is not true.

All data will be treated with the strictest confidentiality, only by authorised personnel and for the sole purpose of investigating, processing and, where appropriate, resolving the possible incident or irregularity reported.