Information management procedure

SUAN FARMA

25 July 2023

Index

1. Purpose and scope 3
2. Subjective scope of application 3
3. Objective scope of application 4
4. Procedure 5
4.1. Communication 5
4.2. Acknowledgement of receipt and initial assessment of communication 6
4.3. Investigation procedure 7
4.4. Conflict of interest 7
4.5. Resolution 8
4.6. Information to the informant 8
5. Right to privacy, honour and self-image and the protection of personal data 8
6. Preservation of documentation 9
7. Confidentiality of information and documentation 10
8. Internal and/or external audits 10

1. Purpose and scope

Suan Farma Holding, S.L. (hereinafter, "**Suanfarma**" or the "**Company"**) has an Internal Information System (hereinafter, the "**IIS**") in order to uphold its corporate values and protect its ethical culture.

In development of the IIS Policy and the principles described therein, this **Information Management Procedure** (hereinafter, the "**Procedure**") constitutes the Suanfarma and its Group's Whistleblower Channel, known as the Ethics Channel (hereinafter, the "**Channel**") as the preferred channel for reporting ethical concerns regarding possible irregularities and/or breaches, in accordance with the provisions of Directive (EU) 2019/1937 of 23 October 2019 of the European Parliament and of the Council on the protection of persons who report breaches of Union law, as well as with Law 2/2023 of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption, which transposes it into Spanish law.

This Procedure, together with the IIS Policy and the appointment of the Committee responsible for it, make up Suanfarma's IIS, in accordance with the provisions of the aforementioned Law 2/2023.

The companies of the Suanfarma Group may adapt the Procedure in order to adapt the provisions of this Procedure to their own specificities, whether by subject matter, jurisdiction (legal requirements) or the relevance of the risk in the subsidiary. In any case, the integration of this Policy in the subsidiaries must be proportionate and aligned with this Procedure.

2. Subjective scope of application

This Procedure applies to:

a) The members of the board of directors and management of the Suanfarma Group, including non-executive members, if any.

b) Any employee or other professional of the Company and of the Group, including trainees, trainees in training, as well as those whose employment relationship has not yet commenced where information on breaches has been obtained during the recruitment process or pre-contractual negotiation.

c) Any person working for or under the supervision and direction of contractors, subcontractors and suppliers of the Company and the Group.

d) The legal representatives of the employees in the exercise of their functions of advising and supporting the informant.

e) Natural persons who, within the organization in which the informant provides services, assist the informant in the process.

f) Natural persons who are related to the informant and who may suffer reprisals, such as co-workers or relatives of the informant.

g) Legal persons for whom the informant works or with whom he/she has any other type of relationship in an employment context, or in which he/she has a significant shareholding - significant being understood as a shareholding that enables the person to have influence over the legal person.

The different protection measures provided for in this Procedure, as well as in the Policy, will be exercised, as appropriate, on all complainants, related third parties and persons affected by the communication of a concern through the Channel. Notwithstanding the foregoing, where specific Procedures exist, they shall be integrated into this Procedure and IIS, for the relevant purposes.

3. Objective scope of application

The persons included within the subjective scope of the ISS may report through the procedure set out in **Section 4** below any conduct or fact that could imply:

- Infringements of European Union law concerning, inter alia, public procurement; financial sector; prevention of money laundering and terrorist financing; product safety and conformity; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety, animal health and animal welfare; public health; consumer protection; protection of privacy and personal data, and security of networks and information systems, financial interests of the Union and internal market.

- Serious or very serious criminal or administrative offences, including offences involving financial loss to the Treasury or Social Security or in matters of health and safety at work.

- Violations of Suanfarma's Code of Ethics and Conduct and any other internal policy or procedure implemented.

The use of this Procedure must be in accordance with the requirements of good faith and must be used rigorously and in a serious and responsible manner. The Channel may not be used for illegitimate, personal or unlawful purposes or in breach of good faith. If it is confirmed that a member of the Company and/or Group has made a false communication, this conduct may be subject to disciplinary proceedings in accordance with the provisions of the Suanfarma Sanctioning Regime and the applicable collective bargaining agreement, without prejudice to any other responsibilities, including those of a criminal nature, that may have been incurred.

No member of Suanfarma and/or the Group may be subject to any disciplinary procedure for communicating facts or conduct that they may have believed to be in breach of the Company's minimum ethical standards, provided that their communication and actions are based on good faith, ethical behavior and, in general, the conviction that they were acting correctly.

In this sense, disciplinary measures may also be adopted that are applicable in accordance with Suanfarma's Sanctions Regime, the collective agreement and other corresponding labour legislation, in the event that, when a conduct that could generate a risk of criminal or administrative charges is known, it is not duly reported.

4. Procedure

4.1. Communication

The procedure is initiated by nominative or anonymous communication by the following means:

- Website of each of the Group's companies.
- Group Intranet in the following section "Ethics Channel".
- At the request of the informant, made through any of the above channels, it may also be submitted by means of a face-to-face meeting within a maximum period of seven (7) days.

  Minutes of the meeting shall be taken and signed by the attendees and shall be accompanied by either an accurate and complete transcript of the conversation or a recording of the conversation in a secure, durable and accessible format. The subject shall be informed in advance that the conversation will be recorded.

In those cases in which the communication is sent to the Committee Responsible for the IIS through alternative communication channels to the above, such communications shall be treated and managed in the same way as those sent through the authorized channels, and therefore this Procedure shall also be applicable to such communications.

In any case, regardless of the manner in which the communication was received, strict observance of the principles of confidentiality, presumption of innocence and the right to defence and the right to honour shall be guaranteed throughout the process for all those involved in the investigation, as well as for the actions carried out in the management and processing of the same.

Once a report has been made, the informant is under a duty of secrecy regarding the report made, the identity of the person or persons to whom the report refers and the facts and documentation that are the subject of the report. He/she must also be fully available to cooperate with the Responsible Committee of the IIS throughout the process of investigating the facts reported.

Notwithstanding the above, anonymity may not always be guaranteed, as there will be occasions when the identity of the person making the communication must be provided due to legal requirements - communication of the facts to the judicial or administrative authority. However, apart from these exceptional cases, the identity of the reporter will not be disclosed, and the reporter will always be protected from any reprisals that may be directed against him or her as a result of his or her communication.

Communications made by reporters shall, to the extent possible, contain the following information:

- Detailed description of the facts reported, always taking into account criteria of truthfulness, objectivity and completeness.
- When the reported events occurred, indicating whether it is a specific date or a period of time.
- How the reported facts came to light.

- Where the reported events took place (work/project site).
- Whether the facts previously reported have been brought to the attention of any member of the Company.
- Whether other members of Suanfarma are known to have knowledge of the reported facts.
- If there is evidence of the reported facts.

Without prejudice to his or her rights under data protection regulations, the informant shall be given the opportunity to verify, rectify and agree to the transcription of the conversation by signing it.

Upon receipt of the communication, the Responsible Committee of the IIS shall include the information in the Information Register, collecting all relevant information contained in the communication so that it is duly recorded.

Likewise, the persons to whom the Policy applies may report to the Independent Authority for the Protection of the informant, A.A.I. or to the competent regional authorities or bodies and, where appropriate, to the institutions, bodies and agencies of the European Union, the commission of any actions or omissions that may involve a breach or irregularity included in the scope of application of this Procedure, either directly or after prior communication through the Company's internal channels.

4.2. Acknowledgement of receipt and initial assessment of communication

Once a communication has been received, the IIS Committee or the Internal Information System Manager shall acknowledge receipt of the communication within a maximum of seven (7) calendar days and shall proceed to its immediate analysis and verification.

The IIS Committee, through the Internal Information System Manager, after carrying out a preliminary analysis and verification of the communication, may consider or reject the communication based on the criteria of sufficiency and relevance, and for this purpose may request additional information or documentation from the communicant that may be relevant to determine the above.

In the event of a rejection, the Committee responsible for the IIS, through the Internal Information System Manager, shall inform the informant of this decision, stating the reasons for the rejection.

On the other hand, in the event that it is upheld, the Committee responsible for the IIS, through the Internal Information System Manager, will inform the Informant, thereby initiating the phase of analysis of the communication.

The IIS Committee shall include in the Register of Information the reasons for both upholding and rejecting the communication.

The Internal Information System Manager may be assisted by personnel from the legal department, from the department concerned, and in the case of subsidiaries located outside Spain, by the personnel of the subsidiary company, if he/she deems it necessary to carry out a proper investigation of the complaint, maintaining in all cases the confidentiality of the file.

4.3. Investigation procedure

The investigation procedure shall be initiated as soon as the Responsible Committee of the IIS accepts a communication submitted by the above-mentioned means and shall have a maximum duration of three (3) months, which may be extended for a further three (3) months when the complexity of the facts or the investigation is sufficiently justified.

The following provisions must be complied with in this process:

- It shall be ensured that the person concerned is informed of the acts or omissions attributed to him or her when it is deemed most appropriate for the purpose of ensuring the proper conduct of the investigation. They also have the right to be heard at any time.

  Strict observance of the principles of confidentiality, presumption of innocence and right to honour, right of defence, prohibition of retaliation and the principle of good faith, as set out in the IIS Policy for all parties involved, will also be ensured throughout the investigation process.

- If deemed necessary, additional information on the submission may be requested from the Reporting Person and, if deemed appropriate, further communication may be held with the Reporting Person, if possible.

- The person concerned shall have the right of access to the file under the terms set out in the applicable legislation, preserving his or her identity and guaranteeing the confidentiality of the facts and data of the procedure.

- In addition, interviews may be held with other members of the Company who may be able to provide additional information to the investigation, for example, witnesses to the events reported.

- The Company may seek the advice of external experts to advise and assist it during the investigation process. Such external experts shall be subject to the same principles and obligations as provided for in this procedure with regard to confidentiality and data protection, and the corresponding agreements shall be signed to that effect.

4.4. Conflict of interest

The filing of a complaint that directly affects persons who may actively participate in its processing, investigation or qualification, whether a member of the Responsible Committee of the IIS or any person collaborating in the processing or investigation, will entail their automatic exclusion during the entire process of investigation and analysis until its resolution, in order to avoid any type of conflict of interest, and to guarantee the objectivity and independence of the actions carried out within the framework of this procedure.

4.5. Resolution

The IIS Committee shall conclude the investigative procedure by issuing an opinion of conclusions (hereinafter referred to as the "**Opinion**"), which shall contain appropriate reasoning for the decision taken and may include, inter alia, a **proposal** to:

a) Open disciplinary proceedings against the offender under the collective bargaining agreement applicable to the offender if it is concluded that the offender has engaged in conduct that could constitute an employment offence.

b) Open disciplinary proceedings against the reporter under the applicable collective agreement if it is concluded that his or her conduct in reporting the facts or behavior could have breached good faith.

c) Adopt corrective measures to prevent the facts or conduct from recurring within Suanfarma.

d) Report the facts or conduct to the appropriate judicial or administrative authorities.

e) Where the facts may be suspected of constituting a criminal offence, the Committee responsible for the IIS system shall immediately forward the information to the Public Prosecutor's Office. If the facts affect the financial interests of the European Union, it shall be referred to the European Public Prosecutor's Office.

f) Take no action as there has been no conduct in breach of the rules.

4.6. Information to the informant

The reporter will be informed by the IIS Committee of the outcome of his or her communication.

The information provided may not contain the details of the investigation carried out or refer to specific persons, but must be stated in general terms, taking into account the confidential nature of the information and the rights of third parties, including, but not limited to, the alleged offender.

5. Right to privacy, honour and self-image and the protection of personal data

The right to privacy, honour and self-image of all persons participating or involved, directly or indirectly, in the proceedings established in this procedure shall be guaranteed at all times and at all times.

In communications made during the procedure, a file number shall be used, omitting in any case any identification of the persons involved.

All persons involved in the proceedings arising from this procedure shall be under an obligation of secrecy (duty of confidentiality) regarding the data and information to which they have had access during the processing of this procedure. Any breach of this obligation shall be punishable by law.

In all cases, the provisions of the data protection regulations in force at any given time shall be complied with in respect of all persons involved in the actions established in this procedure. The Company makes available to its management personnel and its employees and third parties the Privacy Policy which will regulate the processing of personal data collected and processed in connection with the use of the Channel.

Access to personal data processed on the occasion of a communication shall be limited exclusively to those who carry out the internal control and compliance functions or, where appropriate, to the data processors who may be responsible for these functions. There are two exceptions to this limit: first, where access by other persons, or even disclosure to third parties, is necessary for disciplinary measures to be taken or for any legal proceedings to be conducted; second, where disciplinary measures may be taken against an employee, in which case access shall be granted to staff with human resources management and control functions.

6. Preservation of documentation

All documents that may serve as evidence of the conduct or facts that are the subject of the communication must be kept for as long as there is a risk of a criminal offence or there is a legal obligation to keep such documents. Under no circumstances may personal data be kept for a period of more than ten (10) years.

Any tangible or intangible medium containing sufficiently precise and relevant information to be able to determine that a suspected criminal conduct is taking place and to identify the persons involved in such conduct or the department of the Company within which such conduct is taking place shall be considered as a document.

In particular, documents or records which provide adequate evidence shall be kept for possible use in any investigation or analysis in the event of an investigation being initiated by an administrative or judicial body, the Public Prosecutor's Office, the Ombudsman, the Court of Auditors or any other similar body or body with investigative functions:

a) The risk behaviors presumed to have been detected.
b) The interveners.
c) The Impact Opinions.
d) Communications generated in the course of the procedure.
e) All internal and external reports issued, internal memos, e-mails exchanged between members of the Company regarding the incident, etc.
f) The minutes of the IIS Committee in which information related to reported or detected incidents is recorded.

The period of custody shall begin to run as soon as the corresponding opinion is issued. In any case, the filing system must ensure the adequate management and availability of the documentation, both for the purposes of internal control and to meet the requirements of any authorities or public bodies and entities covered by the applicable regulations in due time and form.

Documents shall be stored on optical, magnetic or electronic media which guarantee their integrity, confidentiality, the correct reading of the data, their non-manipulation and their adequate conservation and location. This is without prejudice to the fact that they may also be stored on paper.

In the event that an electronic communication management system is in place, the data of the person making the communication and of the members of the Company and/or third parties shall be kept in the whistleblowing system only for the time necessary to decide whether to initiate an investigation into the reported facts. In any event, three (3) months after the data have been entered, they must be deleted from the Whistleblower Channel environment. If it is necessary to keep them in order to continue the investigation, they may continue to be processed in a different environment.

The obligation to block or retain data provided for in the data protection regulations in force at any given time does not apply to these systems, without prejudice to the cases of retention set out in this Policy. Therefore, complaints that have not been processed may only be retained in an anonymised form or, where appropriate, they will be destroyed or deleted.

7. Confidentiality of information and documentation

All persons who have knowledge of the information and documentation communicated through the Channel are obliged to keep it confidential.

Failure to comply with this obligation may lead to the initiation of disciplinary proceedings in accordance with the collective agreement and other applicable legislation applicable to the offender.

8. Internal and/or external audits

This Procedure and the obligations contained herein may be subject to periodic internal and/or external audits to monitor compliance.

Prepared by	Suanfarma Group
Date	25 July 2023
Version	1.0