Internal Information System Policy

SUAN FARMA

25 July 2023

Index

1. Introduction

The Board of Directors of Suan Farma Holding, S.L. (hereinafter, "**Suanfarma**" or the "**Company"**), in accordance with its commitment to current legislation and the highest ethical and professional standards, has drawn up and approved this Corporate Policy on the Internal Information System (hereinafter, the "**Policy**").

Through this Policy, the Suanfarma Group complies with the requirements of Law 2/2023 of 20 February on the protection of persons who report regulatory infringements and the fight against corruption (hereinafter "**Law 2/2023**"), adopted as a result of the transposition of 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.

2. Object

This Policy is the core element of the Suanfarma Group's Internal Information System and, together with the Information Management Procedure (hereinafter, the "**Procedure**"), seeks to provide the Company and the Suanfarma Group with the resources and principles of action required to promote the use of the Ethical Channel (hereinafter, the "**Channel**") and to ensure the rights of all parties involved, particularly the guarantee of confidentiality, the prohibition of reprisals, the right to defence and the right to honour and the presumption of innocence of those affected by the communications.

At Suanfarma, the Information Management Procedure will be called "**Ethics Channel**".

3. Scope of application

This Policy and the rest of the Internal Information System, including the Procedure (hereinafter, the "**IIS**") in which it is integrated, is of a corporate nature and, consequently, is applicable to all the companies of the Group (hereinafter, the "**Suanfarma Group**").

The companies of the Suanfarma Group may adapt this Policy, either by means of their own policy or by means of an addendum, in order to adapt the provisions of this Policy 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 Policy.

From a subjective point of view, this Policy applies to:

a) The members of the Board of Directors of the Suanfarma Group, including non-executive members where applicable, as well as all members of management.

b) Any employee of the Company and of the Group, including trainees, employees undergoing training period, as well as those whose employment relationship has not yet commenced when the information on infringements they intend to report 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 Suanfarma 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 one that allows the person to have the capacity to influence the legal person.

4. Scope of protection

This Policy protects against any retaliation against any natural or legal person who makes legitimate use of the Channel for the purpose of reporting any actions or omissions that may constitute an infringement:

(i) European Union law,
(ii) serious or very serious criminal or administrative offences, including, but not limited to, all offences involving financial loss to the Treasury or Social Security, or occupational health and safety.

The protection afforded by this Policy and the other elements of the IIS shall not exclude the application of the rules relating to criminal prosecution, and is without prejudice to the protection provided by labour law on occupational health and safety for persons reporting occupational health and safety violations.

5. Declaration of principles

The IIS will be the preferred channel for reporting any non-compliance within its scope of application and will be governed by the following principles of operation and management:

1. **Effectiveness and accessibility**: the SII must ensure that communications are easy to formulate, and that they are presented and managed effectively, so that the entity itself is the first to know of any possible irregularity.

2. **Independence**: all those involved in the management of the IIS must offer a guarantee of independence, in particular the IIS Steering Committee, in such a way that any possible conflicts of interest or personal or professional ties that could affect the good judgement

or credibility of those involved in the communications management process are beyond suspicion.

3. **Confidentiality**: the SII will be designed and managed in such a way as to guarantee the confidentiality of the identity of the informant, the persons affected and any third party mentioned in the communications, as well as the actions carried out in the management and processing of the same. The register of communications supervised by the Committee responsible for the SII shall be regulated in such a way as to guarantee not only the protection of personal data, but also the due restriction of access to unauthorised personnel.

4. **Presumption of innocence and right to honour**: the persons concerned shall have the right to the presumption of innocence and the right to defence, so that under no circumstances may a presumption contrary to the person concerned be assumed when investigating or deciding on a communication submitted.

   To this end, the persons concerned shall have the right of access to the file under the terms of Law 2/2023, to receive the same protection as informants and to be heard and be able to present allegations in the internal investigation procedure whenever they deem it appropriate.

5. **Prohibition of retaliation**: Retaliation against anyone who reports or cooperates in a communication or information process within the scope of protection of this Policy is expressly prohibited.

   Retaliation shall mean any act or omission prohibited by law or which, directly or indirectly, results in unfavourable treatment that places the person who suffers it at a particular disadvantage in the employment or professional context solely because of his or her status as a whistleblower or because of his or her cooperation in the handling of information.

   By way of example, the following conduct may be considered as retaliation:

   a) Suspension of employment contract, dismissal or termination of employment or non-renewal - unless within the regular exercise of managerial authority under labour law.

   b) Damage, including reputational damage, economic loss, coercion, intimidation, harassment or ostracism.

   c) Negative references to professional work.

   d) Blacklisting or dissemination of information in a sector that hinders access to or promotion in the workplace.

   e) Refusal or cancellation of permits or training.

6. **Principle of good faith**: in the same way that the imposition of reprisals is prohibited, Suanfarma will not allow the use of the SII for illegitimate, personal motives or contrary to good faith.

   In the event of misuse of the SII by any reporting person or third party involved, such action may result in the imposition by the Company of the corresponding disciplinary sanction, if applicable, or the exercise of civil or criminal actions that may be pertinent.

6. Committee responsible for the ISS

In compliance with its obligations related to the supervision and promotion of the IIS, the Board of Directors of Suanfarma has appointed the Committee responsible for the SII, whose members will hold office indefinitely.

The members of the Committee responsible for the IIS shall be the Chief Executive Officer/Group Managing Director, the Human Resources Director and the Legal and Compliance Director; and the Head of the Internal Information System shall be the person holding the position of the Legal and Compliance Director.

The appointment and removal of each of the members of the Committee and of the natural person individually designated as the person in charge of delegating responsibility shall be notified to the Independent Authority for the Protection of the Informant, A.A.I., within the following ten (10) working days, specifying, in the case of their removal, the reasons that have justified it.

The Head of the Internal Information System 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.

The IIS Steering Committee shall perform its functions independently and autonomously from the other bodies of the entity and in accordance with the specifications contained in its charter. These functions include:

- Promote and monitor the implementation and effectiveness of this Policy on an ongoing basis.

- Guarantee access to this Policy to all Suanfarma members and interested third parties.

- Implement procedures to manage communications received through the Channel.

- To hear, investigate and issue reports on investigations arising from communications received through the Channel.

- To inform Suanfarma's Board of Directors of the most relevant results of the Channel's activity within the framework of its *reporting* tasks.

7. Publicity of the Channel

In accordance with the provisions of Law 2/2023, Suanfarma has published on its website, in a separate and easily accessible section, access to the Channel and to this Policy.

The Company undertakes to ensure that this Policy and the existence of the Channel are duly disseminated, providing all members of the entity and third parties linked to its professional activity with the necessary information and, where appropriate, training on the subject, to ensure free access to them and all the tools of the SII by which to assert their legitimate rights.

Irrespective of the access to this Suanfarma Channel, any whistleblower may also contact the Independent Authority for the Protection of Whistleblowers.

8. Data protection

From the point of view of personal data protection, the main aspects that apply within the framework of the SII are provided for in Title VI of Law 2/2023 and are detailed below:

- The processing of personal data arising from the application of Law 2/2023 shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPD GDD), in Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, and in Title VI of Law 2/2023, as well as any other applicable law.

- Personal data shall not be collected where it is manifestly not relevant to the processing of specific information or, if collected by accident, shall be deleted without undue delay.

- Processing of personal data necessary for the implementation of Law 2/2023 shall be considered lawful.

- As the Company is an entity obliged to have an SII, the processing of personal data, in cases of internal communication, shall be considered lawful by virtue of the provisions of articles 6.1.c) of the GDPR - the processing is necessary for compliance with a legal obligation applicable to the data controller - and 11 of Organic Law 7/2021, of 26 May.

- Where the processing of special categories of personal data is carried out for reasons of essential public interest, it may be carried out in accordance with Article 9(2)(g) of the GDPR.

- When personal data is obtained directly from data subjects, they will be provided with the information referred to in articles 13 of the RGPD and 11 of the LOPD GDD as established in the privacy policy that regulates the IIS and the Channel.

- Informants and those who make a public disclosure shall also be expressly informed that their identity will in any case remain confidential and that it will not be communicated to the persons to whom the facts related or to third parties.

- The person to whom the facts reported relate shall in no case be informed of the identity of the informant or of the person who made the public disclosure.

- Data subjects may exercise the rights referred to in Articles 15 to 22 of the GDPR.

- In the event that the person to whom the facts related in the communication or to whom the public disclosure refers exercises the right to object, it shall be presumed, in the absence of proof to the contrary, that there are compelling legitimate grounds for the processing of his or her personal data.

- The IIS shall not obtain data that allow the identification of the informant and shall have appropriate technical and organizational measures in place to preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and to any third party mentioned in the information provided, especially the identity of the informant in the event that he/she has been identified.

- The identity of the informant may be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority only in the context of a criminal, disciplinary or disciplinary investigation.

- The processing of the data by other persons, or even their communication to third parties, shall be lawful when this is necessary for the adoption of corrective measures in the Company or the processing of any procedures that may be required.

- Access to the personal data contained in the SII shall be limited to the Responsible Committee and, where appropriate, to whomever the Responsible Committee may authorize for this purpose.

  The Data Protection Officer can be contacted at the following e-mail address: dpo@suanfarma.com

9. Approval and review

The Board of Directors is the competent body to approve this Corporate Policy, the first version of which was approved on 25 July 2023.

This Policy will be reviewed annually or when legislative changes make it necessary.

Prepared by	Suanfarma Group
Date	25 July 2023
Version	1.0