INTERNAL INFORMATION SYSTEM POLICY AND INFORMATION MANAGEMENT PROCEDURE OF SANLUCAR FRUIT S.L.U.

Approved by the Sole Administrator of Sanlucar Fruit S.L.U. on 15 January 2024.

1. DESCRIPTION OF THE DOCUMENT

1.1. Object of the Document

On 21 February 2023, Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, was published in the Official State Gazette (BOE). With the approval of this law, Directive (EU) 2019/1937 of the Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law is transposed into Spanish law.

The purpose of this law is to protect people who, in a work or professional context, detect certain breaches of regulations and report them through the internal information channels that must be set up for this purpose, providing adequate protection against any type of reprisals.

Therefore, in accordance with the provisions of the aforementioned Law, the general regulatory framework is updated to the new legal provisions on the protection of reporting persons, by establishing this Internal Information System Policy (respectively, the "**Policy**" and the "**Information System**").

The purpose of this Policy is to define the principles and premises that regulate the internal reporting system, as well as its procedure, which is intended to provide adequate protection against reprisals that may be suffered by individuals who report any of the actions or omissions that may constitute infringements in the terms defined in the previous section.

The internal reporting system is configured as a tool to strengthen the information/communication culture as an essential mechanism for the prevention, detection and correction of threats to the public interest and regulatory breaches, to consolidate the integrity risk monitoring framework and to facilitate compliance with internal regulations in particular.

The information provided by people who are part of Sanlucar Fruit S.L.U. ("**Sanlucar**") or act in close proximity to it is a valuable source in achieving the aforementioned prevention and detection.

1.2. Approval and validity

This Document, approved by the Sole Administrator on 15/01/2024. The validity of this Document is from the date of publication until a new version is available that cancels it.

1.3. Collectives with access to the internal information system

The following persons (any of them individually or jointly referred to as the "**Informant**") may make use of the communication channels:

(i) any employee, shareholder, participant, member of the administrative, management or supervisory body of Sanlucar (including non-executive members);

(ii) any other person or entity that has any professional relationship with Sanlucar (freelancers, agents, contractors, subcontractors, suppliers, mediators, or any person working for or under the supervision and direction of the above, etc.);

(iii) any other person who has obtained information about infringements in the context of an employment or statutory relationship that has ended, volunteers, trainees, trainees in training, whether or not they are paid, former employees;

(iv) persons whose employment relationship has not yet started, in cases where information on infringements has been obtained during the selection process or pre-contractual negotiation;

(v) legal representatives of the employees in the exercise of their functions of advising and supporting the informant; and

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

Any person who, as an employee of Sanlucar or having adhered to its internal regulations, has knowledge or well-founded suspicions of the commission of a reportable event, is obliged to report it through the corresponding Communication Channel.

1.4. Communication Channels

This Policy integrates the following communication channels (the "**Communication Channel**" or the "**Communication Channels**"):

(i) Compliance Communication Channel: the purpose of the Compliance Communication Channel is to receive written or verbal information related to the following matters:

(a) Actions or omissions that may constitute a serious or very serious criminal or administrative offence, including non-compliance with the obligations provided for: (a) in the set of internal rules, procedures and policies that make up Sanlucar's criminal risk prevention system - including the Sanlucar Code of Conduct - and (b) in the general regulations applicable in this area to Sanlucar's activity.

(b) Actions or omissions which could constitute an offence under the **Annex I**.

(ii) Complaints and Suggestions Channel: The purpose of the Complaints and Suggestions Channel is to receive suggestions, comments, recommendations or reports in writing or verbally.

(iii) Harassment Channel: the purpose of the Harassment Channel is to receive written or verbal reports of situations of sexual harassment as defined in the "Guide for the Equality Committee".
-Sexual and moral harassment" prepared by Sanlucar.

The foregoing matters shall be defined as the "**Policy**" for the purposes of this Policy and the accompanying procedure, the disclosure of facts as the "**Communication**" or "**Communications**" and the content of the Communications as the "**Information**" or "**Information**".

1.5. Responsible for the Information System

The Board of Directors of Sanlucar and of all the other companies to which this Policy applies have appointed a collegiate body (the "**System Manager**") to be responsible for the management of the Information System, by virtue of the resolution adopted on 15/01/2024.

In all matters relating to the application of the provisions governing the operation of the Information System, the System Manager shall carry out his or her functions independently and autonomously from the rest of the Sanlucar bodies, may not receive instructions of any kind in their exercise and must have all the personal and material means necessary to carry them out.

The powers to manage the Information System and the processing of any investigation files that may need to be initiated have been delegated to the President of the collegiate body, by virtue of the resolution adopted by said body on 15/01/2024 (the "**Delegate**").

Sanlucar shall notify the competent authorities of the designation of the body as System Manager within 10 working days of its appointment. It shall also notify its cessation when appropriate, specifying in this case the reasons that have justified the cessation. For the purposes of the first appointment of the System Manager, this period shall be computed from the creation of said authorities and shall follow the procedure to be developed in the regulations.

1.6. Confidentiality

All parties and persons involved in the management and investigation of the Communications received within the framework of the Information System will guarantee the confidentiality of the identity of the Informant, of any third party mentioned in the Communication and of the actions carried out in the management and processing of the same, as well as data protection, preventing access by unauthorised personnel. Sanlucar will ask the person in question to sign a document in which he/she will be given specific instructions regarding his/her actions, as well as the obligation of confidentiality. A draft of the document to be signed by the persons concerned is attached as **Annex II.**

Without prejudice to the foregoing, the identity of the Reporting Person may only be disclosed when required by a judicial authority, the Public Prosecutor's Office or other competent administrative authority within the framework of a criminal, disciplinary or sanctioning investigation. If so requested, the System Manager shall: (i) record such request; and (ii) inform the Reporting Person of such request, provided that such information does not jeopardise the investigation or judicial proceedings.

Failure to comply with the duty of confidentiality shall be considered a very serious offence in accordance with the regulations in force, without prejudice to the disciplinary sanctions that such non-compliance may entail in employment proceedings.

1.7. Whistleblower rights and guarantees for their protection in Sanlucar

The Informant shall enjoy protection, even in situations where Information is provided anonymously, but where the Informant may subsequently be identified. The right to protection will arise only in those cases in which the Informant has reasonable grounds to believe that the Information is truthful at the time of the Communication and provided that it has been made in accordance with the formalities provided for in this Policy and the accompanying procedure.

Specifically, the measures for the protection of the Informant will consist of:

(i) Prohibit any form of retaliation, negative consequence, or threat of retaliation or attempted retaliation against the Reporting Person for making a Disclosure. Without being exhaustive, and by way of example only, the following conduct shall be considered retaliation:

  (a) Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract after the probationary period, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion or denial of promotion and any other substantial modification of working conditions and failure to convert a temporary employment contract into a permanent one, where the employee had legitimate expectations that he/she would be offered a permanent job; unless these measures were carried out as part of the regular exercise of managerial powers under the relevant labour or public employee statute legislation, due to circumstances, facts or breaches that are proven and unrelated to the submission of the communication.

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

  (c) Negative evaluation or references regarding work or professional performance.

  (d) Blacklisting or dissemination of information in a particular sectoral area, which hinders or prevents access to employment or the contracting of services.

  (e) Refusal of training.

  (f) Discrimination, or unfavourable or unfair treatment.

(ii) Exempt the Reporting Person from any liability arising from making a Disclosure, or from acquiring or accessing Information, provided that there are reasonable grounds to believe that it was necessary to make such a Disclosure in order to disclose an act or omission in violation of the Regulations. This disclaimer of liability shall not affect any criminal liability that may attach to the Reporting Person as a result of his or her conduct.

The measures for the protection of the Reporting Person may also apply: (i) to the legal representatives of working persons in the exercise of their functions of advising and supporting the Reporting Person; (ii) to natural persons assisting the Reporting Person in the framework of the procedure for handling Information; (iii) to natural persons who are related to the Reporting Person and who

(iv) legal persons for whom the Reporting Person works or with whom the Reporting Person has any other relationship in an employment context, or in which the Reporting Person has a significant shareholding. Where applicable, a written record should be made of any protective measures that may be applied in respect of third parties other than the Reporting Person.

Notwithstanding the foregoing, Whistleblowers shall not be exempted from liability for acts or omissions that are unrelated to the Communication, or that were not necessary to disclose a violation. Likewise, the above protection measures shall not apply to persons who have reported or disclosed: (i) Information that has already been inadmissible through any other internal communication channel; (ii) Information relating to interpersonal conflicts or affecting only the Reporting Person and the persons to whom the Communication refers; (iii) Public information or information that is considered to be mere rumour; and (iv) Information that does not refer to the Regulations.

The submission of false or misrepresented communications, in bad faith or abuse of rights, may constitute a very serious infringement of the regulations in force, giving rise, where appropriate, to the corresponding disciplinary responsibilities.

1.8. Rights and obligations of the person concerned

The natural and/or legal person to whom the facts that are the subject of a Communication relate and to whom certain actions or omissions that may constitute a breach of the Regulations are attributed (the "**Affected Person**") shall be considered to be affected.

The Affected Party shall have the right to be informed of the actions or omissions attributed to him/her and to be heard at any time during the investigation in case it is initiated, always saving the good purpose of the investigation. The Affected Party shall also have the right to be informed of any decisions Sanlucar may take as a result of the investigation.

At any time during the investigation, the Affected Party may: (i) state his or her full version of the facts, both verbally and in writing; and (ii) provide the investigation with any documents or testimonies he or she deems appropriate for the clarification of the facts. The Affected Party's allegations made verbally shall be documented following the same formalities as those provided for verbal Communications.

The Affected Party shall appear before the investigator(s) when required to do so and shall have the right to the presumption of innocence, to a defence (and may be assisted by a lawyer), to access to the essential elements of the investigation file (provided that such knowledge does not conflict with other rights and legitimate interests of third parties), as well as to the same protection established for Informants, preserving their identity and guaranteeing confidentiality.

The Affected Person shall not: (i) threaten, coerce or attempt to influence any person who is cooperating with the investigation; nor (ii) destroy, tamper with or alter any document, data or information for the purpose of obstructing the investigation.

The Affected Party shall maintain absolute confidentiality regarding the existence of the investigation and its content. Sanlucar will notify the Affected Party of a document in which he/she will be given specific instructions regarding his/her actions and will be informed of the obligation of confidentiality. A draft of the document to be notified to the persons concerned is attached as **Annex III.**

In the event of non-compliance with the obligations described above, the Affected Person may be subject to the appropriate disciplinary sanction.

1.9. Rights and duties of persons called to cooperate with the investigation

All members of Sanlucar are called upon to cooperate with an investigation if requested to do so. The mere fact of collaborating with the investigation can never be a reason for any sanction or reprisal.

In particular, they shall comply with the following provisions:

(i) Appear for interviews to which they may be called, answering the questions put to them.

(ii) Respond to internal requests for information or documentation.

(iii) Provide all the documents that serve to accredit the Information.

(iv) Maintain absolute confidentiality about the existence of the investigation and its content, without disclosing its existence to any third party. Sanlucar will notify the person concerned of a document giving them specific instructions on how to act and informing them of the obligation of confidentiality. A draft of the document to be notified to the persons concerned is attached as **Annex IV.**

Failure to comply with the above obligations may result in disciplinary liability.

1.10. Protection of personal data

The personal data provided on the occasion of a Communication and obtained as a result of the corresponding internal investigation (the "**Personal Data**") will be processed by the personnel provided for in article 32 of Law 2/2023, of 20 February, designated for this purpose within Sanlucar and solely for the investigation of the facts Communicated, the basis that legitimises this processing of Personal Data being that provided for in article 30 in relation to compliance with the legal obligations described in article 10, both of the aforementioned Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption.

As a consequence of the internal investigation procedure, it is possible that in certain circumstances and as explained above, it may be necessary to outsource the investigation work, and therefore there may be access to Personal Data by a third party in the capacity of data processor. Sanlucar guarantees at all times that the choice of these third parties is made with the maximum guarantees in terms of data protection and that the corresponding processing commissioning agreement is signed in accordance with Article 28 of Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**").

The Personal Data obtained during the internal investigation procedure may be communicated, subject to the legal safeguards established, to the judicial authority, the Public Prosecutor's Office or the competent administrative authority within the framework of a criminal, disciplinary or sanctioning investigation.

Personal Data subjects may exercise their rights of access, rectification, erasure, restriction, portability, objection and the right not to be subject to a decision based solely on automated processing (where applicable in accordance with the provisions of the personal data protection regulations) by sending an e-mail to the address: rgpd@sanlucar.com However, the exercise of such rights by the reported person shall not entail the Informant's identification data being communicated to him/her, as his/her identity shall in any case be reserved by virtue of the provisions of Articles 31 and 33 of Law 2/2023 of 20 February. Likewise, the owners of the Personal Data may file a complaint with the Spanish Data Protection Agency. Without prejudice to the foregoing, the holder of the personal data may first contact the Data Protection Delegate designated by Sanlucar, via the e-mail address rgpd@sanlucar.com.

Personal data relating to Information and internal investigations shall be kept only for the period of time necessary and proportionate for the purposes of complying with the applicable regulations, as well as
(i) the data processed may be kept in the information system only for the time necessary to decide whether to initiate an investigation into the facts reported; if it is established that the Information or part of it is not truthful or relevant, it must be immediately deleted as soon as this circumstance comes to light, unless this lack of truthfulness may constitute a criminal offence, in which case the Information shall be kept duly blocked for the time necessary during the legal proceedings; (ii) after three months have elapsed since receipt of the Communication without any investigation having been initiated, the Communication shall be deleted, unless the purpose of retention is to leave evidence of the operation of the system. Communications that have not been acted upon may only be recorded in anonymised form, without the obligation to block being applicable; and (iii) in no case may the data be retained for a period of more than ten years.