Sisal Whistleblowing Policy

Approved by Sisal Board of Directors on 19/10/2022

Table of contents

FOREWORD

The Sisal Group (hereinafter also the “Group” or “Sisal”) is committed to conducting its business activities with honesty and integrity, maintaining the highest standards of ethical conduct and behaviour.

With the aim of promoting and reinforcing these standards, the Group has implemented a Whistleblowing Policy (hereinafter also the “Policy”) for the reporting of any conduct, including omissions, which constitutes or may constitute a violation or inducement to a violation of laws, regulations, values and principles sanctioned by the Sisal Code of Ethics and Conduct, the 231 Model or company policies and procedures, as better specified in the paragraph “PURPOSE AND SCOPE”. Anyone is invited to promptly report such conduct in the manner described below, refraining from undertaking autonomous initiatives of analysis and/or investigation.

For this reason, the Company has implemented specific communication channels for the management of Whistleblowing Reports (as defined below) in order to comply with Directive (EU) 2019/1937 and Law no. 179/2007, which supplements Legislative Decree no. 231/2001 concerning the administrative liability of entities.

To this end, this Policy:

- defines the scope of the Reporting process;
- identifies the persons who may make Reports;
- identifies the channels through which the Report may be made, appropriate to guarantee the confidentiality of its content;
- identifies and prescribes the principles and general rules governing the Reporting process, as well as the consequences of any abuses in the use of the established channels;

- defines the Reporting management process in its various phases, identifying roles, responsibilities, operating methods and tools used;
- defines the modalities of data processing of the content of the Report, including the identification data of the Whistleblower and the Reported Party;
- protects the Whistleblower against retaliatory and/or discriminatory conduct, direct or indirect, for reasons related to the Whistleblowing.

PURPOSE AND SCOPE

This Policy describes the process and communication channels to be used for sending, receiving, analysing and processing Reports of unlawful conduct, including omissions, which constitute or may constitute:

a) a violation or inducement of a violation of laws and regulations relating to the following areas:
   - public procurement;
   - financial services, products and markets and the prevention of money laundering and terrorist financing;
   - safety and conformity of products;
   - consumer protection;
   - protection of privacy and protection of personal data and security of networks and information systems;
   - public health;
   - environmental protection;
   - violations of competition and state aid rules;
   - violations of corporate tax rules;

b) a violation or inducement of a violation of domestic law, such as:
   - values and principles laid down in the Sisal Code of Ethics and Conduct;
   - values, principles and controls identified in the Organisation, Management and Control Model pursuant to Legislative Decree 231/2001 of Sisal;
   - internal policies and procedures.

DEFINITIONS AND ABBREVIATIONS

WHISTLEBLOWER: Subject, among those referred to in paragraph “RECIPIENTS OF THE POLICY”, who makes the Report.

REPORT: Communication by the Whistleblower concerning information on Unlawful Conduct.

UNLAWFUL CONDUCT: Any act or omission constituting or likely to constitute a violation or inducement of a violation with respect to the conduct set forth in paragraph “PURPOSE AND SCOPE”.

REPORTED PARTY: Subject to whom the Whistleblower attributes the Unlawful Conduct that is the subject of the Report.

CHANNELS FOR REPORTING: Communication channels identified by Sisal as the means, internal or external to the organisation itself, for transmitting reports.

RETALIATION: Acts of retaliation or discrimination, direct or indirect, against the Whistleblower for reasons directly or indirectly linked to the Report, by the Company.

SUPERVISORY BOARD: Supervisory Board pursuant to Legislative Decree 231/2001 and direct recipient of the reports pursuant to Legislative Decree 231/01 as amended by Law 179/2017 "Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship".

PARTIES RESPONSIBLE FOR RECEIVING THE REPORT: Supervisory Board and Whistleblowing Committee.

WHISTLEBLOWING COMMITTEE: Committee composed of Internal Audit Director and the Chief Risk & Compliance Officer.

RECIPIENTS OF THE POLICY

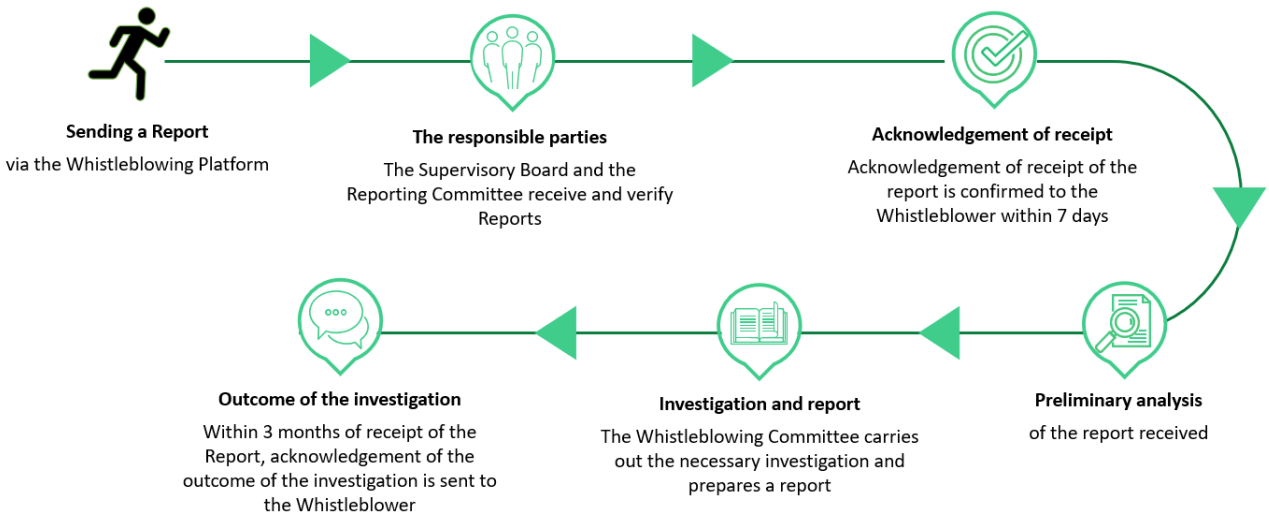
This Policy applies to the following persons (hereinafter also referred to as "Recipients" and/or "Whistleblowers"):

a) Group workers (employees, self-employed, volunteers, paid and unpaid trainees, former employees[1], job applicants[2]);
b) shareholders and members of the administrative, management or supervisory board of an enterprise, including non-executive members, volunteers and paid and unpaid trainees;
c) any person working under the supervision and direction of contractors, subcontractors and suppliers, customers, partners, consultants and, more generally, the Group's stakeholders.

[1] If they report or disclose information on violations acquired in the context of the terminated employment relationship.

[2] If their employment relationship has not yet commenced and information concerning the breach has been acquired during the selection process or in pre-contract negotiations.

THE REPORTING PROCESS



Reporting unlawful conduct

Sisal encourages the persons referred to in paragraph “RECIPIENTS OF THE POLICY“ to submit Reports concerning unlawful conduct, even if only potential, of which they become aware.

If a Whistleblower has a reasonable suspicion that unlawful conduct has occurred or may occur, he/she may report this by using the Whistleblowing Platform (the “Platform”) or, alternatively, by ordinary mail, to the address “Whistleblowing Service”, Via Ugo Bassi, 6 - 20159 Milan. Although Whistleblowing Reports may also be made anonymously, Sisal recommends that they be nominative, in order to allow the persons in charge to carry out a more efficient investigation, applying in any case the protections provided against possible retaliation. This applies, in particular, to Reports received by ordinary mail, where the Whistleblower is required to provide a contact or address for subsequent communications.

The Platform, on the other hand, makes it possible to handle any communications and/or requests subsequent to the Report, even if these are made anonymously.

The Report must be based on precise and concordant facts and made in good faith. The Whistleblower must provide all the elements in its knowledge, useful to proceed with the due and appropriate verifications to confirm the validity of the facts reported. The Report must be accompanied by any useful documentation supporting the potential unlawful conduct that is the subject of the Report.

It is particularly important that it includes, where these elements are known to the Whistleblower:

- a detailed description of the facts that occurred and how they became known;
- date and place where the event occurred;
- name and role of the persons involved or elements that might enable them to be identified;
- names of any other persons who may report on the facts that are the subject of the Report or elements that may enable them to be identified;
- reference to any documents that may confirm the accuracy of the reported facts.

The Whistleblower should take care not to report information that is irrelevant or unnecessary to the Report.

All Reports are received by the following parties (hereinafter also referred to as “the parties responsible for receiving Reports”), who are appointed as authorised processors and duly instructed on the processing of personal data pursuant to Articles 29 and 32, paragraph 4 of Regulation (EU) 2016/679 and Article 2-quaterdecies of Legislative Decree 196 of 2003:

a) Supervisory Board, direct recipient of the reports pursuant to Legislative Decree 231/01;
b) Whistleblowing Committee, consisting of:

a. Internal Audit Director;
b. Chief Risk and Compliance Officer.

Depending on the type of offence reported, whether relating to the Model pursuant to Legislative Decree no. 231/2001 or other types of offence (e.g. internal fraud, corruption and/or other offences to the detriment of Sisal), the investigations are coordinated by the Supervisory Board or the Whistleblowing Committee, respectively.

Reports concerning situations of an exclusively personal nature and outside the scope of the provisions of the law is not taken into account.

Moreover, if the Whistleblower makes a report, he/she may be held liable in cases where the report proves to be, due to wilful misconduct or gross negligence, false, unfounded and/or made for the sole purpose of harming the Reported Party. In more serious cases (e.g. wilful misconduct in the falsehood of the report), the conduct may be subject to disciplinary proceedings pursuant to Law 300/70 or cause termination of the contract or appointment.

Whistleblowing Platform

The Whistleblowing Platform ensures traceability of the workflow of the Report.

All information in the Report is protected to ensure the outmost confidentiality and is accessible only by the persons responsible for receiving the Report or by persons expressly authorised by them.

The Platform is made available to the Recipients of the Policy through the Sisal website (Speak Up!) or via the company intranet. When a Report is sent, after having read the privacy policy on the processing of personal data, the Whistleblowing Platform issues a token (Report ID), which can be used by the Whistleblower to obtain information on the outcome of the Report and to ensure that communications are also completely anonymous.

Furthermore, the Whistleblowing Platform provides for the possibility for the Whistleblower to exclude internal Functions from the management of the Report, if they are directly involved in the Report. For further details on the management of conflicts of interest, please refer to the dedicated section of this Policy.

The persons responsible for receiving Reports access the Platform to consult all the Reports received and carry out verification activities. Their accesses are tracked and the Platform is protected by appropriate technical security measures.

Reports received outside the prescribed channels

The Sisal Department receiving a Report that has been forwarded outside the prescribed channels must forward it without delay, in original with any attachments, to the parties responsible for receiving Reports, i.e. the Supervisory Board (which can be contacted at the email address odv.sisal@sisal.it) and the Whistleblowing Committee. The transmission should be made in accordance with the criteria of utmost confidentiality and in such a way

as to protect the Whistleblower and the identity of the persons reported, without prejudice to the effectiveness of the subsequent investigations. No copies of the Report received and forwarded to the responsible parties should be made.

Preliminary analysis

Reports are subject to preliminary analysis by the Whistleblowing Committee, with the coordination of the Supervisory Board in cases falling within its remit.

The Whistleblowing Committee (hereinafter the "Committee") verifies the presence of useful data and information to allow an initial assessment of the Report. Within 7 (seven) days of receiving the Report, the Committee sends the Whistleblower an acknowledgement of receipt of the Report, using the communication methods adopted by the Whistleblower.

The Committee takes all necessary measures to treat Reports in a confidential manner, also with a view to protecting the identity of the Whistleblower, the Reported Party and the other persons mentioned in the Report.

In the course of its verifications, the Committee may avail itself of the support of the corporate functions competent from time to time and, where deemed appropriate, of external consultants specialised in the field of the Report received and whose involvement is functional to the investigation of the Report, ensuring the confidentiality and anonymisation of any personal data contained in the Report.

All parties involved in the investigations must maintain strict confidentiality regarding information received during the inspections.

At the end of the preliminary analysis, the Committee, with the coordination of the Supervisory Board in cases within its competence, may:

a) archive the Report as not sufficiently supported by evidence, manifestly unfounded or relating to conduct or facts not relevant to this Policy;
b) open the investigation phase referred to in the next paragraph.

The Committee informs the Whistleblower of the outcome of its investigations within a reasonable time limit, in any case not exceeding 3 (three) months or 6 (six) months in duly justified cases.

Investigation

With reference to each Report, where, following the preliminary analysis, useful and sufficient elements emerge or can be deduced to make an assessment of the merits of the Report, the Committee shall:

- initiate specific analyses, involving, where appropriate, the corporate functions concerned by the Report;
- terminate the investigation at any time if, in the course thereof, it is established that the Report is unfounded;
- check the possible legal implications for the Company;
- assess whether there is an obligation to inform the authorities;
- in the event that the conduct complained of continues, request precautionary measures to be taken to bring the conduct to an end.

In addition, the Committee must:

- ensure that the investigation is accurate, fair, impartial and protects the confidentiality of the identity of the Whistleblower and of the persons involved, including the Reported Party;

- ensure that appropriate measures are taken for the collection, processing and storage of personal information, and ensure that the needs of the investigation are balanced with the need to protect privacy. On this point, it is the duty of the Whistleblowing Committee, in agreement with the Supervisory Board in cases falling within its remit, to assess the possibility of informing the Reported Party of the investigation. The Reported Party is, in any case, always informed by the Whistleblowing Committee in case of initiation of disciplinary proceedings;
- ensure that the investigation is carried out with the utmost speed and diligence.

Outcome of the investigation

At the end of the verification phase, the Committee prepares a report summarising the investigations carried out and the evidence that emerged, and shares it, on the basis of the results, with the parties from time to time competent, including the Supervisory Board, in order to define any intervention plans to be implemented and the actions to be taken to protect the Group, also communicating the results of the investigations and verifications carried out in relation to each Report to the heads of the corporate structures concerned by its contents.

The Committee classifies, within the Whistleblowing Platform, the analysed Report as follows:

1. Report lacking sufficient and relevant information;
2. Report unfounded;
3. Report founded.

Should the conclusion of the analysis reveal the absence of sufficiently circumstantiated elements or, in any case, the groundlessness of the facts referred to in the Report, the latter is filed by the Committee, together with the relevant reasons.

It is understood that, in all cases, upon completion of the verification of the merits of the Report received, the Whistleblower is provided with feedback within a reasonable time limit, in any case not exceeding 3 (three) months or 6 (six) months in duly justified cases.

CONFLICT OF INTEREST

The handling of the Report must be entrusted exclusively to persons who are not in a situation of conflict of interest. Therefore:

a) if the Report refers to one or more members of the Committee, the members who are in a situation of conflict of interest does not take part in the handling of the case and the remaining members of the Committee have to identify other suitable persons to restore the integrity of the Committee;

b) if the Report or the conflict of interest situation concerns all the members of the Committee, the Report must be addressed to the members of the Supervisory Board, who will assess how the Report should be handled;

c) if the Report refers to one or more members of the Supervisory Board, the Supervisory Board itself shall inform the Board of Directors, which shall assess the operational procedures to be followed and the corporate Functions to be involved in the management of the Report.

These provisions also apply in the event that the conflict arises during the course of the inspection.

PROTECTION OF THE WHISTLEBLOWER AND THE REPORTED PARTY

Protection of the Whistleblower

Following a Report, the protection and confidentiality of the identity of the Whistleblower is ensured at all times, by processing the data in accordance with the law and all useful measures being taken to prevent the dissemination of the Whistleblower's data and the content of the Report.

Sisal guarantees that the identity of the Whistleblower is not disclosed - without his/her explicit consent - to anyone who is not part of the authorised personnel competent to receive and follow up the reports, unless disclosure is a necessary and proportionate obligation imposed by EU or national law.

Retaliatory or discriminatory acts, whether direct or indirect, against the Whistleblower for reasons directly or indirectly linked to the Report are prohibited and sanctioned.

Sisal guarantees the prohibition and removal of the effects of any form of retaliation against the Whistleblower, including in particular:

- dismissal, suspension or equivalent measures;
- relegation in rank or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training;
- demerits or negative references;

- the imposition or administration of disciplinary measures, reprimand or other sanction, including a fine;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- the failure to convert a fixed-term employment contract into a permanent employment contract where the employee had legitimate expectations of being offered permanent employment;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or financial loss, including loss of economic opportunities and loss of income;
- blacklisting on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- early termination or cancellation of the contract for goods or services;
- cancellation of a licence or permit;
- submission to psychiatric or medical examinations.

It should also be noted that measures for the protection of Whistleblowers also apply, where appropriate:

a) to facilitators (i.e. those who assist the Whistleblower in the reporting process);

b) third parties connected with the Whistleblower and who might risk retaliation in a work context, such as colleagues or relatives of the Whistleblower;

c) legal entities that the Whistleblower owns, works for or is otherwise connected to in a

work context.

The Whistleblower shall not be held liable for defamation, breach of copyright, breach of secrecy obligations, breach of data protection rules and breach of trade secret disclosure. No liability can be attributed to the Whistleblower even in relation to the conduct adopted to access the information that is the subject of the Report. This is without prejudice to cases where the report proves to be false and made with malice or gross negligence. In addition, the parties concerned have the right to legal protection in the event of criminal or civil liability on the part of the Whistleblower in connection with the falsity of what has been declared or reported.

Protection of the Reported Party

In order to avoid detrimental consequences within the work context, even if only of a reputational nature, the protection reserved to the Whistleblower, as set out in the preceding paragraph, should also be granted to the Reported Party.

After investigating whether the Report is well-founded, the Committee, if disciplinary proceedings are opened, informs the person to whom the Report relates and keeps him/her up-to-date on developments in the proceedings, compatibly with the performance of the necessary verification and evidence-gathering activities, so as to enable him/her to exercise his/her right of defence.

The Reported Party's personal data may be forwarded to the competent administrative or judicial authorities and, more generally, to public bodies, in compliance with the formalities laid down by law, or in order to comply with requests received from them.

REPORTS

On a quarterly basis, the Committee provides the CEO with a report summarising the reports handled (filed and investigated), containing the results of the analysis, including the adoption (or non-adoption) of disciplinary measures.

PROCESSING OF PERSONAL DATA

It should be noted that the personal data of the Whistleblower, the Reported Party and all the persons involved in the Report are processed in accordance with the current legislation on the protection of personal data set out in Regulation (EU) 2016/679 ("GDPR") and Legislative Decree 196/2003, as amended by Legislative Decree 101/2018. In particular, it is highlighted in this context that:

- the processing activities underlying the management of the Report are carried out in compliance with the principles laid down in Articles 5 and 25 of the GDPR;
- the Whistleblower receives, before sending the Report, a notice pursuant to Article 13 of the GDPR specifying the purposes and methods of the processing of its personal data and the period of retention thereof, the categories of recipients to whom the data may be transmitted in the context of the management of the Report and the rights recognised to the Whistleblower by the GDPR; the Reported Party is also provided with a notice pursuant to Article 14 of the GDPR in accordance with the obligations of secrecy and confidentiality imposed by Legislative Decree No. 231/2001, as amended by Law No. 179/2017, as well as in view of the risk of making it impossible or seriously prejudicing the achievement of the purposes of the processing related to the reports made under the whistleblowing system (see Article 14, paragraph 5, letters b) and d) of the GDPR);
- as indicated in the privacy policies provided to data subjects, personal data are processed for the time necessary to achieve the purposes justifying their collection and processing (e.g. evaluation and management of the Report) and subsequently deleted or anonymised according to the defined retention periods;
- appropriate technical and organisational measures are put in place to ensure the security of personal data, in accordance with the legislation in force, both during the transmission

of the Report and during the analysis, management and archiving of the Report;

- the exercise of the rights by the Whistleblower or the Reported Party (the “data subjects” within the meaning of the privacy legislation), in relation to their personal data processed within the Whistleblowing process, may be limited, pursuant to and for the purposes of Article 2-undecies of Legislative Decree 196/2003 as amended by Legislative Decree 101/2018, in the event that an actual and concrete prejudice to other interests protected by specific regulatory provisions may result from such exercise, with the clarification that under no circumstances may the Reported Party be allowed to make use of his/her rights to obtain information on the identity of the Whistleblower;
- access to personal data is granted only to the persons responsible for and authorised to receive such Reports, limiting the communication of confidential information and personal data to third parties only when necessary.

RECORD KEEPING

In order to ensure the reconstruction of the different stages of the process, the Committee shall ensure:

1. the traceability of Reports and their receipt, filing, investigation and assessment;
2. the storage of the documentation relating to the Reports and the related verification activities, as well as any decision-making measures taken by the competent functions, in appropriate files and with the appropriate levels of security/confidentiality;
3. the retention of documents and reports for the period of time prescribed by law and in any case in compliance with the applicable data protection legislation.

The functions involved in the activities of verifying the validity of the Report ensure, each to the extent of its competence, the traceability of the data and information and provide for the storage and archiving of the documentation produced so as to enable the reconstruction of the different stages of the process.

PARTY RESPONSIBLE FOR UPDATING THE POLICY

The Anti-Corruption & Compliance Function is responsible for this Policy and ensures that it is regularly updated.

DISSEMINATION AND COMMUNICATION OF THE POLICY

The Company shall inform all Recipients of the Policy of its existence and content by publishing it on the Sisal Intranet and website.

TRAINING

The Human Resources Function, with input from or in consultation with the Anti-Corruption & Compliance Function, is responsible for planning and delivering training activities relating to the Policy and for ensuring its availability and communication.