Fosber Group

Whistleblowing Policy

HISTORY OF MODIFICATIONS			
VERSION	**DATE**	**PREPARED BY**	**DESCRIPTION**
01.00	14/11/2023	Fosber HR Dept	First draft

VERIFICATION AND APPROVAL PROCESS	
Prepared by	Fosber HR Dept
Checked by	ODV Fosber
Approved by	Fosber CEO

1 Introduction and scope

Whistleblowing' is the term used to identify a report made by a person who, in the course of his or her duties, becomes aware of an offence, risk or dangerous situation that could harm the company he or she works for, as well as customers, colleagues, citizens and any other category of subjects.

FOSBER, sensitive to ethical and proper business conduct issues, has implemented a system to receive and manage reports of actions, facts or situations that may constitute unlawful conduct with respect to:

- legislation in force;
- Code of Ethics;
- Organisation, Management and Control Model pursuant to Lgs D 231/01;
- Occupational Safety Management System;
- Environmental Management System;
- Alleged violations of regulations and laws in the performance of work activities that may cause damage or harm, even if only in terms of image, to the Company.
- EU Regulation 679/2016 (GDPR)

The Whistleblowing Policy adopted by ***FOSBER*** intends:

- to ensure the confidentiality of the whistleblower and in the spirit of the rule, protect him/her from possible retaliation;
- to promote a culture based on responsibility and ethics;
- to allow ***FOSBER***'s Corporate and Control Bodies to be informed of facts or conduct contrary to the adopted ethical principles, in order to identify and manage possible deficiencies in the internal control and risk management system;
- to provide guidelines for making and handling reportseffectively, responsibly and in compliance with the law.

This Policy identifies:

- subjects that can make a report;
- the acts or facts that may be reported, as well as the requirements that reports must meet in order to be taken into account;
- the modalities through which alleged violations can be reported and the persons in charge of receiving the reports;
- the process of inquiry and possibly investigation when a report is made;
- the protocols put in place to ensure the confidentiality of the personal data of the reporting party and the reported case;
- the protocols put in place to ensure the protection of the personal data of the reporting party and of any reported person;
- the protocols put in place to ensure the prohibition of retaliation and the prohibition of discrimination against the Reporting Party.

Lastly, the document aims to ensure that Whistleblowing management activities are carried out in compliance with the principles of professionalism, transparency and fairness, in accordance with the provisions of Legislative Decree 24/2023 (Legislative Decree on whistleblowing) and, more generally, with the applicable laws and regulations, as well as in compliance with the company's Code of Ethics and the Organisation, Management and Control Model pursuant to Legislative Decree 231/2001.

This Policy has been drafted with reference to:

- Decree-Law No. 24 of 10/3/2023 - Implementation of EU Directive 2019/1937 [...] concerning the protection of persons who report breaches of Union Law and [...] of national laws
- Organisation, Management and Control Model pursuant to Legislative Decree 231/01 concerning the Administrative Responsibility of ***FOSBER*** Bodies
- EU Regulation 679/2016 (GDPR)

For matters not explicitly dealt with in this Policy and/or for interpretation, reference is made to Legislative Decree 24/2023.

This Policy applies both in Fosber S.p.A. and in all companies directly or indirectly controlled by it and belonging to "Fosber Group", subject to the EU Directive 2019/1937.

2 Definitions and glossary

Internal Channel	This refers to the instrument adopted by ***FOSBER*** and Fosber Group companies subject to the EU Directive 2019/1937 to enable the submission of reports of possible violations of laws, regulations, rules or procedures. The internal channel adopted by ***FOSBER*** and the companies of Fosber Group guarantees, through the application of encryption tools, the confidentiality of the identity of the reporting party and his or her personal data, as well as the content of the Report and related documents
Legislative Decree 24/2023	This refers to Legislative Decree 10 March 2023 no. 24 'Implementation of EU Directive 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 and laying down provisions for the protection of persons who report breaches of national laws"
EU Directive 2019/1937	This refers to EU Directive 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 and laying down provisions for the protection of persons who report breaches of national laws*"
Domicile of the Reporting Management Team	This refers to the domicile elected by the Reporting Management Team at Fosber SpA, Via Provinciale per Camaiore 27/28 - 55064 Monsagrati (LU)
Facilitator	A natural person who assists a reporting party in the reporting process, operating within the same work context and whose assistance must be kept confidential.
Fosber Group - Group	this refers to Fosber itself and all companies controlled, directly or indirectly, by Fosber within the meaning of art. 2359 of the (It.) Civil Code).
Fosber or Company	Fosber SpA – Sede in Monsagrati (LU) 55064, Via per Camaiore 27/28, Tax code and VAT IVA 00429870462
Reporting Management Team	This is the team responsible for the management of Confidential Reports for FOSBER SpA and the companies of Fosber Group (in the latter case, the Reporting Management Team operates pursuant to art. 5 of It. Legislative Decree 24/2023). It manages and is responsible for the proper management of the Internal Channel, the Investigation (Triage) phase and the Compulsory Investigation. The Reporting Management Team consists of a committee composed of two independent and autonomous professionals with cross-disciplinary expertise in legal and compliance matters and the Manager of the HR Department.
Reporting Party or Whistleblower	This is the party making the report.
Customer	Disclosure of any breach of regulations that may impact the Company made in accordance with the terms of this Policy and in compliance with the principles and rules set out in Legislative Decree 24/2023

Retaliation	Any conduct, act or omission, even if only attempted or threatened, committed by reason of the report or public disclosure and which causes or may cause the reporting person or the person making the report, directly or indirectly, unjust damage.
Reported Party	This refers to the person who is the subject of the Report
MyWhistleblowing ***FOSBER*** and ***QUANTUM***	Platform dedicated to the management of Confidential Reports in accordance with the requirements of Legislative Decree 24 of 10 March 2023. The MyWhistleblowing Fosber platform can be accessed via the website www.fosbergroup.com or directly at https://areariservata.mygovernance.it/#!/WB/FOSBER The MyWhistleblowing Quantum Corrugated platform can be accessed via the website www.quantumcorrugated.com or directly at https://areariservata.mygovernance.it/#!/WB/QUANTUMCORR
Competent corporate body	This refers to the Corporate Body, the Body or the Office to which the Reporting Management Team reports the results of the conducted activities. It is the party responsible, by virtue of its competence, for taking any remedial measures or providing corrective action.
Fosber Group Company	This refers to Fosber SpA and any of its subsidiaries affected by EU Directive 2019/1937

3 Actors involved

The body responsible for the management of the Internal Channel of each Company of Fosber Group is the Reporting Management Team, expressly appointed by each of the aforementioned Companies and authorised to perform the activities deemed necessary for the performance of the tasks assigned by Legislative Decree 24/2023 and by this Policy. The Reporting Management Team consists of a committee composed of two independent and autonomous professionals with cross-disciplinary expertise in legal and compliance matters and the Manager of the HR Department. For the purposes of this Policy, the committee constituting the Reporting Management Team must guarantee, in its operation, autonomy, independence, professionalism and specific competence.

The Reporting Management Team may avail of the support of internal structures of each Fosber Group company deemed to be more competent with respect to the case being reported.

In the event of conflict of interest, i.e. those cases in which the Reporting Management Team is also the Reporting Party, with the reported party or is otherwise a person involved or affected by the Report (such a conflict may, e.g., also exist with respect to the external subject, if the management of the platform is outsourced), the Report should be addressed to one of the members of the Fosber Board of Directors or the Board of Statutory Auditors by means of a notice sent to the registered office of the Company, in a closed and confidential envelope for the attention of the Board of Directors or of the Board of Auditors in the person of the chosen member, who will take care of sharing its contents with the members of the Reporting Management Team who are not involved in the Report.

This is without prejudice to the right to opt for the so-called 'external' reporting under article 6 of Legislative Decree 24/2023.

Pursuant to article 4, sixth paragraph, of Legislative Decree 24/2023, if the Report has to be communicated to a person other than the Reporting Management Team (e.g. the Supervisory Board or the Board of Statutory Auditors), the latter must forward it to the Reporting Management Team within seven days of receipt, and at the same time inform the Reporting Management Team.

The persons who can make a Report are as follows ('Reporting Parties'):

- members of the corporate bodies (Shareholders' Meeting, Board of Directors, Board of Auditors, etc.);
- personnel (including current employees, former employees, temporary workers, apprentices, trainees or volunteers in connection with circumstances occurring during the employment relationship or selection process);
- external parties that have relations with the companies of FOSBER Group (so-called stakeholders such as shareholders, customers, suppliers, agents, business associates, partners, contractors, subcontractors, as well as collaborators and employees of the aforementioned parties).

4 Reporting Methods

Each company in Fosber Group has a dedicated**Internal** Reporting**Channel** , which can be activated in the manner described below.

4.1 WRITTEN FORM

a) **"MyWhistleblowing *FOSBER*" platform ,** accessible via the website ww.fosbergroup.com, or directly from https://areariservata.mygovernance.it/#!/WB/FOSBER

'MyWhistleblowing Quantum Corrugated' platform can be accessed via the website www.quantumcorrugated.com or directly at https://areariservata.mygovernance.it/#!/WB/QUANTUMCORR

The platform is outside the company servers, is managed through cloud technologies and is equipped with an encryption tool that guarantees the confidentiality of the reporting party's identity.

Access to the platform is permitted after registration of the user and formal acknowledgement of the privacy statement and Policy.

Anonymous access is permitted.

b) **By postal service in a sealed envelope** (registered **mail**) to the address of the Fosber Reporting Management Team , domiciled at Studio Legale Pascerini e Associati, Via Barberia 6, Bologna, expressly indicating "Whistleblowing Report" on the envelope

4.2 ORAL OR VERBAL FORM

By a verbal report on the messaging system available on the MyWhistleblowing Fosber platform where a voice and text messaging system is activated. It is also possible to request a **personal and confidential interview** with the Reporting Management Team.

Reports or information received by ordinary email, pec (certified email), or delivered in a manner different from the above are not covered by this Policy and consequently cannot avail of the protections provided by the Law[1].

4.3 EXTERNAL CHANNEL

As provided for by the Law, the National Anti-Corruption Authority (ANAC) has activated an 'External' Reporting Channel that the Reporting Party may submit a Report to if, at the time of its submission, one of the following conditions is met:

a) there is no compulsory activation of the internal reporting channel within their work context, or said channel, even if compulsory, is not active or, even if activated, does not comply with the provisions of Article 4 of the Decree;

b) the Reporting Party has already made a Report through the Internal Reporting Channel pursuant to Article 4 of the Decree and the Report has not been followed up;

[1] See Legislative Decree 24 of 10 March 2023

c) the Reporting Party has reasonable grounds to believe that, if he or she made a Report through the Internal Reporting Channel, it would not be effectively followed up, or that the Report might lead to the risk of retaliation;

d) the Reporting Party has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

5 The Report

Any behaviour, act or omission that harms the public interest or integrity of ***FOSBER***, and that integrates (or is justifiably believed to integrate), may be **reported internally** - i.e. through the whistleblowing channel that ***FOSBER*** has decided to adopt (see 4.1 and 4.2 of this Policy):

a) a so-called predicate offence, already relevant under Legislative Decree No. 231/2001;

b) a violation of the Management and Control Organisational Model adopted by ***FOSBER*** pursuant to Legislative Decree No. 231/2001;

c) an infringement of Community and national rules on

- public contract
- financial services, products and markets
- prevention of money laundering and terrorist financing
- product safety and conformity
- environmental protection
- radiation protection and nuclear safety
- food and feed safety
- animal health and welfare
- public health
- consumer protection
- privacy and data protection
- network and information system security

d) a breach of Community rules protecting and guaranteeing the financial interests of the European Union;

e) an infringement of the Community rules designed to protect and guarantee competition and the free movement of goods, persons, services and capital within the European common market;

f) a practice (not non-compliant, but) nevertheless circumventing the Community rules set out in (c), (d) and (e) above;

In the presence of the conditions already set out in paragraph 4.3 of this Policy, only the breaches relevant under Legislative Decree no. 24/2023, i.e. those listed above in letters a) to f), may also be the subject of **external reporting** (i.e. through the whistleblowing channel set up by ANAC).

In any case, Legislative Decree No. 24/2023 expressly provides that mere 'irregularities', i.e. improper conduct that does not, however, amount to an offence or a breach of the regulations listed above, cannot be reported - either through the Internal Channel or through the external channel set up by ANAC.

The Report **must be adequately circumstantiated**[2] and provided with a wealth of details, with elements such as to bring to light facts and situations referable to specific contexts and occurring in the workplace, specifying that no personal data other than those strictly necessary for the management of the Report itself will be collected and that, in the event of accidental collection, these will be immediately deleted by the Reporting Management Team. The Reporting Party is therefore obliged to provide all the available and useful elements to enable the Reporting Management Team to carry out the due and appropriate checks and verifications to ascertain whether the reported facts are well-founded, such as, but not limited to:

i. a clear and comprehensive description of the facts covered by the report;

ii. the circumstances of time and place in which the facts that are the subject of the report were committed;

iii. personal details or other elements allowing the identification of the person(s) who has/have carried out the reported facts (e.g. job title, place of employment where he/she carries out the activity);

iv. any documents supporting the Report;

v. any other information that may provide useful feedback on the existence of the reported facts.

The scope of this Policy **does not include**:

- reports on situations of a personal nature concerning claims or grievances relating to relations with hierarchical superiors or colleagues, as well as relating to the performance of one's work;
- reports based on mere suspicions or rumours concerning personal facts that do not constitute an offence: this is because it is necessary both to take into account the interests of third parties who are the subject of the information reported, and to avoid the Company carrying out internal inspections that risk being unhelpful and in any case costly.

Anonymous reports will only be taken into account if all the elements are present to enable the Reporting Management Team to carry out an independent investigation; otherwise they will be filed.

6 Management of Reports

Once the Report has been received according to the Internal Channel provided for in this Policy through the written or verbal methods described in the previous paragraph, it is handled in the following stages:

6.1 Protocol and custody

If the Report is made through access to the **MyWhistleblowing *FOSBER* web platform** , it is the platform itself that manages the protocol phase through an encryption system and the issuance of a unique identification code in compliance with the relevant legislation.

The encryption key is kept by the Reporting Management Team, who may use it only and exclusively with the express and formal consent of the Reporting Party or by order of the competent judicial authority.

Upon receipt of the Report, no later than 7 days from the date of receipt, the Reporting Management Team, via the platform, sends a notice of receipt and acknowledgement of the Report. The communication is sent via an encrypted communication.

In the case of paper reports, upon receipt of the report, the Reporting Management Team will assign a unique code to the report, which cannot be traced back to the identity of the Reporting Party, and will log the report, precisely identifying:

[2] A report can be considered circumstantiated if it allows the identification of factual elements that are reasonably sufficient to initiate an investigation (e.g.: the offence committed, the reference period and possibly the value, the causes and purpose of the offence, the company/division concerned, the persons/units involved, the anomaly in the control system).

- day and time of reception;
- subject of the report;
- status of the report (to be filled in at each stage of the process, e.g. preliminary investigation, investigation and communication of findings, filing).

Upon receipt of the Report, no later than 7 days from the date of receipt, the Reporting Management Team sends a notice of receipt and acknowledgement of the Report. The communication is sent through the same system used by the Reporting Party, by means expressly authorised by the latter.

The documentation must be collected in a confidential file kept by the Reporting Management Team at the address at which they are domiciled for the purpose of carrying out the task set out in this Policy. It is the duty of the Reporting Management Team to ensure the necessary level of confidentiality of the Reporting Party and to manage all the paper/IT documentation related to the Report received by implementing appropriate technical and organisational security measures.

In the case of a **Report received by telephone or confidential interview**, the documentation and minutes of the meetings/phone call should be collected in a confidential file kept by the Reporting Management Team. It is the duty of the Reporting Management Team to ensure the necessary level of confidentiality of the Reporting Party and to manage all the paper/IT documentation related to the Report received by implementing appropriate technical and organisational security measures.

With regard to the storage of documents, for all matters not provided for in this Policy, reference is made to Article 14 Legislative Decree 24/2023.

6.2 Triage

The purpose of the investigation is to verify the validity and type of the report received. For this purpose, the Reporting Management Team, by carrying out a preliminary screening, will assess the admissibility of the report on its merits, i.e:

- Preliminary determination of the type of offence with respect to the laws in force, the regulations applicable to the Company, the policies or procedures adopted by the Company, etc. (i.e. predicate offences pursuant to Legislative Decree 231/01, violations of privacy laws or the GDPR Regulation, Code of Ethics, safety management system procedures, environmental management, etc.);
- Preliminary assessment of the admissibility of the Report with reference to the subjective qualification of the reporting person[3], the description of the facts and any supporting documents and evidence submitted;
- Identification of the Corporate Body competent for the type of violation reported (i.e. Board of Directors, Board of Statutory Auditors, 231/01 Supervisory Board, DPO, Prevention Employer, HR Manager, etc.);
- The Reporting Management Team considers whether to request further information from the Reporting Party, through the same channel used by the Reporting Party.

Following the investigation, the Reporting Management Team draws up a specific memorandum or record showing the outcome of the investigation phase. The report is recorded in the MyWhistleblowing Fosber platform or in the confidential file.

[3] See art. 3, par. 3 and par. 4 of Legislative Decree 24/2023

6.3 Compulsory Investigation

The Compulsory Investigation is the set of activities aimed at verifying the content of the Reports and at acquiring elements useful for the subsequent assessment phase, **guaranteeing at all stages the utmost confidentiality on the identity of the Reporting Party and on the subject of the Report**.

The main purpose of the Compulsory Investigation is to verify the veracity of the information submitted for investigation, providing an accurate description of the facts established, by means of audit procedures and objective investigative techniques.

The investigation may be carried out by the Reporting Management Team, by individual members of the Reporting Management Team, by assigned persons, by offices of the Company expressly instructed by the Reporting Management Team or by external and independent specialists identified and instructed by the Reporting Management Team.

It is everyone's duty to cooperate with the person in charge of the investigation in the performance of the investigation.

Of each investigation, the appointed person will prepare a final report containing at least:

- the established facts;
- the evidence gathered;
- the causes and shortcomings that allowed the reported situation to occur.

At the end of the investigations, when it is found that the report received is unfounded, the Reporting Management Team files the report and, where possible[4], informs the Reporting Party.

If the report proves to bewell-founded, the Reporting Management Team informs the Body identified in the previous paragraph (ref. "Investigation / Triage") in order to take the necessary actions, defined on a case-by-case basis in relation to the specificity of the situation.

The Compulsory Investigation must be completed within 3 months from the date of receipt of the Report[5]. Upon completion of the compulsory investigation, the Reporting Manager issues a report to the Reporting Party acknowledging the outcome of theinvestigation. The acknowledgement should be transmitted to the Reporting Party using the same reporting channel as for the Report where possible.

6.4 Filing

In order to ensure traceability, confidentiality, preservation and retrievability of data throughout the proceedings, documents are stored and filed via the MyWhistleblowing Fosber platform. If the Reporting Party has used the verbal channel or the paper transmission, the Reporting Management Team shall store it in a special cabinet secured at its Domicile and accessible only to specially authorised and instructed persons.

All documentation will be retained, subject to further legal deadlines in the cases expressly provided for, for 5 years from the date of closure of the activities[6], in accordance with the provisions of Article 14 of Legislative Decree 24/2023, in compliance with confidentiality obligations.

[4] In relation to the channel used for reporting and the use of anonymity by the reporting party

[5] See art. 5, paragraph 1, letter d of Legislative Decree 24/2023

[6] See Art 14(1) of Legislative Decree 24/2023

[7] See Art. 12 Legislative Decree 24/2023

7 Confidentiality and processing of personal data

The **confidentiality** of the Reporting Party's identity is guaranteed, in accordance with the obligations set out in Article 12 paras. 2 et seq. of Legislative Decree 24/2023 during all stages of the process and post-filing. The Reporting Management Team and all persons deemed most competent in the handling of the Report that may be appointed by him/her are bound by the confidentiality of the personal data and circumstances that are the subject of the Report.

The utmost confidentiality is guaranteed with regard to the persons and facts reported, using, to this end, criteria and methods of communication suitable for protecting the identity and honourableness of the persons mentioned in the reports, avoiding in any case the communication of the data acquired to third parties unconnected with the reporting process.

Transmission and communication between the members of the Reporting Management Team and between the Assigned Subjects, if any, is allowed ONLY using the internal communication channels of the MyWhistleblowing ***FOSBER*** Platform. The transmission of documents, information, memoranda or other data by e-mail is NOT permitted. The identity of the Reporting Party, according to the provisions of Article 12 p. 2 of Legislative Decree 24/2023, cannot be disclosed to persons other than those competent to receive or follow up Reports, without the express consent of the person making the Report.

The handling of reports and the related processing of personal data contained therein is carried out in compliance with the provisions of Italian law and European Regulation 679/2016. In the case of reports relating to situations occurring in countries other than Italy or of a reporter not resident in Italy, the report, the data of the reporting party and the associated documentation are in any case processed in accordance with Italian law and European Regulation 679/2016 (GDPR)

Documents, photos, videos, audio recordings sent by the reporting party that may represent a violation of personal data within the meaning of Article 33 GDPR, confidentiality or other personal right, or that have defamatory and libellous content, may be subject to disciplinary measures and/or reporting to the competent authorities.

8 Prohibition of Retaliation and Measures to Support and Protect the Reporting Party

The Reporting Party may not suffer any retaliation as a result of the Report. The prohibition of retaliation is also extended to persons connected to the Reporting Partysuch as Facilitators, family members of the Reporting Party and legal bodies connected to the Reporting Party.

The following conduct, within the meaning of Article 17 of Legislative Decree No. 24/2023, can be construed as retaliation:

- dismissal, suspension or equivalent measures;
- demotion or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- the failure to convert a fixed-term employment contract into a permanent employment contract where the employee had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- inclusion on improper lists 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 the supply of goods or services;
- cancellation of a licence or permit;

- the request to undergo psychiatric or medical examinations.

The Judicial Authority may adopt all the measures, including provisional ones, necessary to ensure the protection of the rights of the reporting party, including compensation for damages, reinstatement in the workplace, an order to cease the conduct in breach of the aforementioned Article 17 of Legislative Decree no. 24/2023 and the declaration of nullity of the acts adopted in breach of said article.

Pursuant to Article 20 of Legislative Decree no. 24/2023, any criminal, civil or administrative liability of the reporting party who discloses or disseminates information on breaches

- covered by the obligation of secrecy is excluded (unless the obligation of secrecy is imposed by national or EU rules on classified information, professional and medical secrecy, secrecy of court decisions)
- relating to copyright protection
- relating to the protection of personal data
- offending the reputation of the person involved or reported

provided that

a) the reporting party, at the time of disclosure or dissemination, had reasonable grounds to believe that
   - the disclosure or dissemination of such information was necessary to disclose the breach
   - the above information was true
   - the breach falls within those provided for by Legislative Decree no. 24/2023 and referred to in paragraph 5 of this Policy
b) the report was made in accordance with the procedures laid down in Legislative Decree No. 24/2023 and referred to in paragraph 5 of this Policy.

However, the criminal, civil or administrative liability of the Reporting Party is not excluded in the event of

   - conduct, acts or omissions not related to the report or not strictly necessary to disclose the breach
   - conduct for the purpose of acquiring or gaining access to information on violations provided for by law as offences.

This is without prejudice to the application of the provisions on the exercise of the right of workers to consult their representatives or trade unions, on protection against unlawful conduct or acts carried out as a result of such consultations, and on the suppression of anti-union conduct.

In any case, the subject that

a) makes, with wilful misconduct or gross negligence, reports that turn out to be unfounded, aimed solely at damaging or prejudicing persons, processes or the Company,
b) makes a report outside the cases and/or methods provided for in Legislative Decree No. 24/2023

lapses from the protection and support measures provided for by Legislative Decree no. 24/2023 and may be subject to disciplinary measures, in line with the relevant CCNL (national collective labour agreement), as well as to further appropriate regulatory actions.

9 Information activity

Each of Fosber Group Companies will take care to share appropriate information on the whistleblowing tool and the provisions of this Policy.

* * * * * *