WHISTLEBLOWER POLICY

	NAME	TITLE	SIGNATURE	DATE
Author	Yumi Charbonneau	Chief Legal Officer		
Reviewer	Vincent Lheureux	Senior Internal Auditor		
Authoriser	Luuk Zonneveld	CEO		

Effective Date:	
Classification	Public

Approved by the Board of Directors on 23rd December 2023

1. Introduction

BIO must take necessary measures to ensure that its activities are conducted in accordance with the law and with the highest degree of ethics and integrity. Improper and illegal actions can cause irreparable harm to BIO and/or its stakeholders and adequate policies and procedures should be put in place to detect, investigate and, where appropriate, pursue legal action against such actions.

BIO has elaborated this whistleblower policy (the "**Policy**") to provide balance and effective protection to staff members and other persons defined herein who report integrity breaches as further set out in this Policy. BIO wishes to foster a culture of good communication and corporate social responsibility within its organization, whereby reporting persons are considered to contribute to self-correction and excellence. Subject to applicable law however, this Policy does not create any obligation to report a breach.

This Policy is established pursuant to the law of 8 December 2022 relating to the reporting channels and the protection of persons who report integrity breaches in the federal governmental authorities and with the integrated police, which transposes the 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.

This Policy is without prejudice to specific procedures and protection regimes applicable in accordance with the law (e.g. laws relating to (sexual) harassment at work).

2. Material Scope - Breaches

2.1 This Policy applies to reports ("**Reports**") relating to the following breaches (the "**Breaches**"):

2.1.1 the following integrity breaches:

(a) any action or failure to act that constitutes a threat to or a breach of the public interest and that:

(i) constitutes a breach of directly applicable European provisions, the laws, decrees, circulars and internal rules and procedures applicable to BIO and its employees; and/or

(ii) constitutes a risk for the life, health or safety of persons or the environment;

(iii) demonstrates a serious shortcoming in the professional obligations or in the proper management of BIO;

(iv) constitutes a breach of BIO's Code of Ethics and Rules of Conduct;

(b) knowingly instructing or recommending committing an integrity breach as listed in paragraph (a) above;

2.1.2 breaches that relate to the following areas:

(a) public procurement, including breaches of BIO's *Procurement Manual*;

(b) financial services, products and markets and prevention of money laundering and terrorist financing, including breaches of BIO's *KYC Policy*;

(c) protection of the environment, including breaches of BIO's *ESG Policy*;

(d) protection of privacy and personal data, and security of network and information systems, including breaches of BIO's *Personal Data Processing Policy*;

(e) prevention of tax fraud;

(f) prevention of social fraud;

(g) product safety and conformity;

(h) radiation protection and nuclear safety;

(i) food and animal feed safety and animal health and well-being;

(j) public health;

(k) consumer protection.

2.2 This Policy is without prejudice to other provisions relating to the reporting of breaches that are stipulated in legal and regulatory provisions and directly applicable European provisions, including the law anti-money laundering law of 18 September 2017 as detailed in BIO's *KYC Policy*. The protection measures referred to in this Policy and the law of 8 December 2022 relating to the reporting channels and the protection of persons who report integrity breaches in the federal governmental authorities and with the integrated police are applicable to the extent they are more favourable.

3. Personal Scope – Reporting Persons

3.1 This Policy applies to the following persons who report a Breach in accordance with this Policy (the "**Reporting Persons**"):

(a) BIO's employees;

(b) persons working on a self-employed basis for BIO;

(c) BIO's shareholder (representative), the members of the board of directors, the General Director of the DGD, the government commissioners and the members of the executive committee;

(d) volunteers and trainees, whether paid or unpaid;

(e) persons who work under the supervision and direction of contractors, subcontractors and suppliers;

(f) persons as listed in (a) through (e) whose relationship has ended (e.g. former employees), with respect to information acquired during said relationship;

(g) persons as listed in (a) through (e) whose relationship has not commenced (e.g. job applicants or tenderers), with respect to information acquired during the recruitment process or other pre-contractual negotiations.

3.2 The protection offered by this Policy further extends to the following persons:

(a) facilitators, i.e. a physical person who assists a Reporting Person in the reporting process in a work-related context and whose assistance is confidential (e.g. confidential counsellors);

(b) third parties who are associated with a Reporting Person and who could suffer retaliation in a work-related context, such as colleagues or family members of a Reporting Person;

(c) legal entities that are the property of Reporting Persons, that employ Reporting Persons or with which Reporting Persons are otherwise associated in a work-related context.

4. Conditions for protection of Reporting Persons

4.1 Reporting Persons qualify for protection under this Policy provided that:

(a) they had reasonable grounds to believe that the information on Breaches reported was true at the time of reporting and that such information fell within the scope of this Policy, as compared to a person in a similar situation with similar knowledge; and

(b) they reported either internally in accordance with article 5 or externally in accordance with article 6, or made a public disclosure in accordance with article 7.

4.2. A Reporting Person will not lose the benefit of the protection provided in this Policy merely as a result of the fact that the Report, provided it was made in good faith, appears to be untrue or unfounded.

4.3. Anonymous Reports are admissible and shall be followed up by the internal and external reporting channels. Persons who reported or publicly disclosed information on Breaches anonymously, but who are subsequently identified and suffer retaliation, shall qualify for the protection provided herein, provided that they meet the conditions provided in article 4.1.

4.4. A person will only be protected pursuant to this Policy provided that Reports are made in good faith in accordance with the terms of this Policy. Reports that do not meet these requirements, contain allegations that are knowingly untrue and are made with the intent to cause prejudice to any person (including BIO), can be subject to disciplinary

action the severity of which will depend on the circumstances, such as the nature of the allegations, the knowledge and intent of the author and whether the allegations were made only internally and/or externally/publicly, and can, subject to applicable laws, lead to dismissal for cause (*ontslag om dringende reden/licenciement pour faute grave*).

5. Internal Reporting and Follow-up

BIO shall seek to build an atmosphere of trust where Reporting Persons feel safe to file Reports through the internal reporting channel provided in this article, where a Breach should be able to be addressed effectively and without fear of retaliation.

5.1. Reports shall be submitted in writing to **the Internal Auditor**, whose details are provided in **Annex 1**.

5.2. Reports shall be sent **by e-mail**, with a description of the Breach in reasonable detail and the relevant factual information and documents in the Reporting Person's possession. The Internal Auditor shall acknowledge receipt of the Report to the Reporting Person within seven (7) days of that receipt.

5.3. The Internal Auditor:

(a) shall diligently follow up on the Reports (including anonymous Report) and will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person;

(b) shall consider the prima facie merits of the Report and information and documents provided. The Internal Auditor can decide that the Report is admissible for further investigation and follow-up or that the Report manifestly lacks merit (e.g. because the facts clearly do not constitute a Breach), in which case they will promptly inform the Reporting Person thereof, along with the reasons for such determination;

(c) shall, upon declaring the Report admissible, diligently follow up on the Report. The Internal Auditor shall carry out an inquiry, the extent of which will depend on the circumstances surrounding the Report and its complexity and shall consider:

(i) the information and documents provided by the Reporting Person;

(ii) information collected from other sources, where appropriate, including internal sources, provided that such actions are not likely to compromise the Reporting Person's position;

(iii) advice from external advisors, at BIO's expense, if necessary;

(d) shall consult on the matter and propose actions and solutions with the relevant Chief, alternatively the CEO or the Chairperson of the Audit Committee (whomever is most appropriate), provided that such consultation is not likely to compromise the Reporting Person's position;

(e) shall, upon closing of the inquiry, prepare a written report with his or her findings, an assessment of the facts and the measures they recommend to BIO's management or to the Chairperson of the Audit Committee, as appropriate, on the proposed course of action, a copy of which shall be provided to the Reporting Person;

(f) shall provide feedback in a reasonable timeframe, not exceeding three (3) months from the acknowledgment of receipt or, if no acknowledgment was sent to the Reporting Person, three (3) months from the expiry of the seven-day period after the Report was made; and

(g) shall provide clear and easily accessible information to the Reporting Person on the procedures for external reports to the competent authorities as provided in Article 6.

5.4. The Internal Auditor shall maintain a register in which each Report is recorded and shall ensure adequate record-keeping of all reported Breaches and related information, to ensure that every Report is retrievable and that information received through the Reports can be used as evidence in enforcement actions where appropriate. All such documents and information are maintained for a period of ten years. However, the personal data contained in such documents and information shall only be maintained for the duration of the inquiry, unless judicial or disciplinary procedures are initiated, in which case such data are maintained for the duration of such procedures.

5.5. The Reporting Person may request a physical meeting (if reasonably possible, otherwise by other direct contact such as by telephone or videoconference) with the Internal Auditor, to be held within a reasonable timeframe from the request.

5.6. The Internal Auditor concludes the inquiry upon completion of the recommended actions.

5.7. The Internal Auditor shall report annually to the Audit Committee on the application of this Policy.

6. External Reporting: the Federal Ombudsman

6.1 The Reporting Person can report the Breach to the external reporting channel:

- after having made a Report through the internal reporting channel; or
- directly, without going through the internal reporting channel.

6.2 The external reporting channel for the Breaches pursuant to this Policy is the Federal Ombudsman. All information on how to file a complaint through the external reporting channel can be found on the website of the Federal Ombudsman: **https://www.federaalombudsman.be/en/centre-for-integrity/whistleblowers**. On this website, the Reporting Person will find all relevant information regarding the role of the Federal Ombudsman, the conditions to benefit from the protection referred to in this Policy, the procedure for the follow-up of Reports, relevant contact details, the remedies and

procedures for protection against retaliation and the availability of confidential advice for persons considering filing a Report and generally all other aspects relating to the external reporting channel and how it deals with Reports.

6.3 The Reporting Person can file a Report with the Federal Ombudsman either in writing or orally. The Report can also be made in person, within a reasonable timeframe. The filing shall contain the following information:

(a) the name and contact details of the Reporting Person, except if the Report is filed anonymously;
(b) the date the Report is filed;
(c) the nature of the employment relationship between the Reporting Person and BIO;
(d) BIO's designation;
(e) a description of the Breach;
(f) the date on or the period during which the Breach took place, is taking place or is very likely to take place.

6.4. The Federal Ombudsman follows up on the Report and:

(a) makes a determination as to its admissibility or to discontinue the process;
(b) if the Report is deemed admissible, opens an inquiry, in which case they inform the CEO or the Chairperson of the Board of Directors thereof, unless there is a suspicion that they are involved in the Breach;
(c) can request staff members to cooperate with the inquiry;
(d) can request any person they deem relevant to provide a statement and any employee of BIO when so requested is required to cooperate with such request;
(e) upon closing of the inquiry, prepares a report with their findings, an assessment of the facts and the measures they recommend, which is sent to the CEO or the Chairperson of the Board of Directors;
(f) informs the judicial authorities if they deem that they have sufficient elements to conclude that a crime or offence has taken place and the CEO or the Chairperson of the Board of Directors is informed thereof;
(g) provides regular feedback to the Reported Person.

6.5 The Federal Ombudsman will however not process complaints relating to the following Breaches:

(a) acts of **harassment, violence at work and inappropriate sexual behaviour at work**, that shall be reported to the internal or external prevention advisors, the details of which are provided in Annexe 2;
(b) acts of **discrimination** based on:
   (i) nationality, so-called race, skin colour, origin or national or ethnic descent;
   (ii) sex, pregnancy, medically assisted procreation, breastfeeding, maternity, family responsibilities, gender identity, gender expression, sex-characteristics and medical or social transition,

   which shall be reported to:

   - UNIA - https://report.unia.be/en/report-it;

- the Institute for Equality of Women and Men (in case of discrimination based on sex) - https://igvm-iefh.belgium.be/en.

Further information on the acts referred to in this article 6.6 and relevant reporting channels is available in BIO's works' regulations (*arbeidsreglement/règlement de travail*).

7. Public Disclosure

A Reporting Person who makes a public disclosure shall be protected pursuant to this Policy if any of the following conditions is fulfilled:

(a) the Reporting Person first reported internally, then externally or directly externally in accordance with articles 5 (*Internal reporting and follow-up*) and 6 (*External reporting – the Federal Ombudsman*), but no appropriate measures were taken in response to the Report within the required timeframe; or

(b) the Reporting Person has reasonable grounds to believe that:

(i) the Breach may constitute an imminent or real danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or

(ii) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the Breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the Breach or involved in the Breach.

8. Confidentiality

The identity of the Reporting Person shall not be disclosed to anyone beyond the staff members competent to receive or follow up on Reports, who shall be required to maintain the confidentiality of the relevant information, without the explicit consent of that person, unless required pursuant to specific legislation where necessary and proportionate in the context of investigations by national authorities or judicial proceedings, including with respect to the safeguard of the rights of the defence of the concerned person. This shall also apply to any other information from which the identity of the reporting person may be directly or indirectly deduced. Any request for access to an administrative document from which the identity of the Reporting Person can be deduced, directly or indirectly, is denied, unless the Reporting Person consents to such access.

The Reporting Person is informed in writing in advance of any disclosure of their identity, and of the reasons therefor, unless such information would endanger related inquiries or judicial procedures.

9. Processing of Personal Data

Any processing of personal data carried out pursuant to this Policy shall be carried out in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation – "GDPR") and the law of 30 July 2018 relating to the protection of natural persons with respect to the processing of personal data.

The purpose of the processing of data following a Report is to receive and follow up on Reports relating to Breaches with a view to verify the accuracy of the allegations made in the Report or publication and to manage the reported Breach.

BIO acts as controller with respect to data processed in connection with internal Reports.

As provided in article 26 of the law of 8 December 2022 relating to the reporting channels and the protection of reporting persons of integrity breaches in federal governmental authorities and the integrated police, in connection with the follow up of Reports pursuant to this Policy, the scope of the obligations provided in articles 14 (*Information to be provided where personal data have not been obtained from the data subject*), 15 (*Right of access by the data subject*) and 16 (*Right to rectification*) is restricted pursuant to article 23, 1, h) GDPR. The scope of articles 14 to 16 GDPR is restricted with respect to the Reporting Person in order to prevent or react to attempts to obstruct, hinder, disrupt or delay the follow up of a Report. The scope of article 14 to 16 GDPR is restricted with respect to any other person than the Reporting Person in order to prevent the obstruction, hindering disruption or delay of the follow up of Reports and of to protect the identity of the Reporting Persons. The restrictions come into force as from the date of the Report and can only be applied to the extent the rights would be prejudicial to the confidentiality of

the inquiry, the follow-up of the Report and the secrecy of the inquiry. The restrictions do not apply to data that are not linked to the object of the inquiry.

10. Protection of Reporting Persons

10.1 Protected persons

The following persons shall be protected from retaliation, threats of retaliation and attempts of retaliation as listed in article 10.2 (the "**Protected Persons**"):

(a) the Reporting Persons;

(b) third parties associated with the Reporting Persons who can suffer retaliation in a work related context, such as colleagues or family members as from the moment they have reasonable grounds to believe that the Reporting Person falls within the scope of this Policy;

(c) facilitators, as from the moment they have reasonable grounds to believe that the Reporting Person falls within the scope of this Policy;

(d) the legal entities that are owned by the Reporting Persons, for which the Reporting Persons work or are otherwise associated in a work related context;

(e) a person who has cooperated with the inquiry by the external reporting channel, and his or her counsel.

10.2 Retaliation measures

Any form of retaliation, threats of retaliation and attempts of retaliation against the persons listed in article 10.1 is forbidden, including:

(a) suspension, lay-off, dismissal or equivalent measures;

(b) demotion or withholding of promotion;

(c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;

(d) withholding of training;

(e) a negative performance assessment or employment reference;

(f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;

(g) coercion, intimidation, harassment or ostracism;

(h) discrimination, disadvantageous or unfair treatment;

(i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that they would be offered permanent employment;

(j) failure to renew, or early termination of, a temporary employment contract;

(k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;

(l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;

(m) early termination or cancellation of a contract for goods or services;

(n) cancellation of a license or permit;

(o) psychiatric or medical referrals.

10.3 Procedure in the event of alleged retaliation

A Protected Person who is of the opinion that they suffer retaliation can file a reasoned complaint with the external reporting channel (**https://www.federaalombudsman.be/en/whistleblower-retaliation-complaint-form**). In such case, the burden of proof of the absence of retaliation rests on BIO.

10.4 Further protections and remedies

(a) A Protected Person further has the benefit of the protections and can exercise the remedies provided in the law of 8 December 2022 relating to the reporting channels and the protection of persons who report integrity breaches in the federal governmental authorities and with the integrated police.

(b) Provided the Reporting Person made the Report or public disclosure in accordance with this Policy and that the Report or public disclosure of the relevant information was necessary to reveal the Breach, as a rule they shall not be liable by virtue of any contractual or legal confidentiality requirement to which they are subject.

11. Protection period and termination

11.1 Commencement of the protection

The protection against retaliation commences as from the date of the filing of the Report, or, with respect to the persons who cooperate with the inquiry by the external reporting channel, as from the date they start their cooperation.

11.2 End of the protection

The protection shall terminate on the date of the closing of the written inquiry report if:

(a) the Protected Person was involved in the Breach;

(b) the Reporting Person knowingly reported untrue information;

(c) the person who cooperated with the inquiry knowingly provided dishonest, untruthful and manifestly incomplete information to the investigators.

11.3 Information

The Reporting Person and the Protected Person are informed in writing of their protection and, if applicable, the termination thereof.

12. Review of Policy

BIO will review this Policy to ensure it remains fit for purpose. The review will be conducted at least every two (2) years, or sooner when necessary as a result of a change in BIO's environment or in the applicable regulatory framework.

ANNEX 1 – INTERNAL REPORTING CHANNEL

1. Internal Auditor

   Vincent Lheureux
   Tel: +32 (0)2 778 99 16
   E-mail: vincent.lheureux@bio-invest.be

ANNEX 2 – REPORTING CHANNELS FOR SPECIFIC ACTS

NOT TO BE REPORTED TO THE FEDERAL OMBUDSMAN

Acts of harassment, violence at work and inappropriate sexual behaviour at work and acts of discrimination shall be reported to the following channels:

(a) Internal Prevention Advisors

Anne Emmerechts
E-mail: Anne.Emmerechts@bio-invest.be
Tel: +32 (0)2 778 99 81

Thomas Destrebecqz
E-mail: Thomas.Destrebecqz@bio-invest.be
Tel: +32 (0)2 897 33 22

(b) Confidential Counsellor

Quentin De Vreese
E-mail: Quentin.DeVreese@bio-invest.be
Tel: +32 (0)477 19 97 64

(c) External Prevention Advisor – SECUREX

Fanny Laridon
Prevention advisor psychosocial aspects
Tel: 0800/100 59 (ext. 1) – Green line
E-mail: health-safety@securex.be

Dr Sonia Sepulveda Carmona
Occupational physician
Tel: +32 (0)2 729 93 18
E-mail: bru.sep@securex.be