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 25 May 2021

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 breaches to the laws and regulations 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 based on international standards on the subject, including recognized corporate governance standards, taking into account the relevant provisions of applicable data protection law, in particular the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") and the Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data ("**the GDPR Implementing Law**") and the recommendation issued by the Data Protection Authority (previously the Privacy Commission) on the subject on 29 November 2006. This Policy further considers the provisions of 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, to be transposed into Belgian law by December 2021.

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. Scope

2.1 This Policy applies to breaches (the "**Breaches**") to:

(a) laws and regulations, and where applicable, internal policies, to which BIO is subject in respect of the following:

(i) public procurement, including BIO's *Procurement Manual*;

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

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

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

(v) fraud, corruption, and other illegal activities;

(vi) competition, State aid, tax;

(vii) labour laws generally, and health and safety laws in particular;

(b) the law of 3 November 2001 relating to the creation of BIO and the Management Agreement entered into with the Belgian State;

(c) BIO's *Code of Ethics and Rules of Conduct*.

2.2 The protection offered by this Policy applies to the following persons (the "Reporting Persons"):

(i) BIO's employees (including temporary staff and trainees);

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

(iii) BIO's directors;

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

(v) persons as listed in (i) through (iv) whose relationship with BIO is yet to begin (e.g. job applicants), with respect to information acquired during the recruitment process or other pre-contractual negotiations.

3. Conditions for protection of Reporting Persons

3.1 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; and

(b) they reported either internally in accordance with article 4 or externally in accordance with article 5, or made a public disclosure in accordance with article 6.

3.2 BIO expressly discourages anonymous reports. Anonymous reports will only be admissible in exceptional circumstances and will be treated with the required level of severity. However, persons who reported or publicly disclosed information on Breaches anonymously, but who are subsequently identified and suffer retaliation, shall nonetheless qualify for the protection provided herein, provided that they meet the conditions laid down in article 3.1.

4. Internal Reporting and Follow-up

4.1 BIO encourages reporting through the internal reporting channels provided in this article before reporting through external channels where the Breach can be addressed effectively internally and where the Reporting Person considers that there is no risk of retaliation.

4.2 Reports shall be submitted in writing to the Internal Auditor or the HR Manager, as deemed most appropriate by the Reporting Person. The details of the internal reporting channels are provided in Annex 1.

4.3 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 or the HR Manager, as applicable, shall acknowledge receipt of the report to the Reporting Person within seven (7) days of that receipt.

4.4 The Internal Auditor or the HR Manager, as applicable:

(a) is competent for following-up on the reports 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 or the HR Manager, as applicable, 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 or the HR Manager, as applicable, 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 proposed actions and solutions with the relevant Chief, alternatively the CEO or 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 formulate recommendations to BIO's management on the proposed course of action;

(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;

(g) 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. Reports shall be stored for no longer than is necessary to comply with the requirements imposed by this Policy, or other requirements imposed by law.

4.5 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 or HR Manager, as applicable, to be held within a reasonable timeframe from the request.

4.6 The Internal Auditor or the HR Manager, as applicable, concludes the inquiry upon completion of the recommended actions.

4.7 The Internal Auditor and the HR Manager shall report annually to the Audit Committee on the application of this Policy.

5. External Reporting

Where:

- the report was not dealt with satisfactorily pursuant to article 4 of this Policy (*Internal reporting and follow-up*), e.g. because the internal channel did not function properly, the report was not dealt with diligently, or no appropriate action was taken to address the Breach despite the results of the related internal enquiry confirming the existence of the Breach; or
- the use of internal channels cannot be expected to function properly, e.g. because the Reporting Person has valid reasons to believe they would suffer retaliation,

the Reporting Person can report the Breach to the appropriate external channel, depending on the nature of the Breach. A non-limitative list of potential external channels is provided in Annex 2.

6. 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 and/or externally in accordance with articles 4 (*Internal reporting and follow-up*) and 5 (*External reporting*), but no appropriate action was 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 manifest 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.

7. 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, without the explicit consent of that person, unless required where necessary and proportionate in the context of investigations by national authorities or judicial proceedings. This shall also apply to any other information from which the identity of the reporting person may be directly or indirectly deduced.

8. Processing of Personal Data

Any processing of personal data carried out pursuant to this Policy shall be carried out in accordance with the GDPR, the GDPR Implementing Law, and BIO's Personal Data Processing Policy. Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

9. Protection of Reporting Persons

Reporting Persons who report Breaches in compliance with this Policy shall be protected from retaliation, threats of retaliation, and attempts of retaliation, including in particular in the form of:

(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.

If BIO takes any of the above actions against a Reporting Person following the report of a Breach (save for (g), (h) and (k), from which BIO shall refrain in any event), it shall be required to provide a satisfactory justification that such action was not due to the Reporting Person reporting a Breach.

10. Consequences of malicious, and frivolous or abusive reports

Reporting Persons will only be protected pursuant to this Policy provided reports are made in accordance with the terms of this Policy. Reports that do not meet these requirements 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 may, subject to applicable laws, lead to dismissal for cause.

11. 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 CHANNELS

1. Internal Auditor

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

2. HR Manager

   Lucie Stramare
   Tel: +32 (0)2 778 99 85
   E-mail: lucie.stramare@bio-invest.be

ANNEX 2 – EXTERNAL REPORTING CHANNELS

1. Reports of violence, or sexual or moral harassment, and other infringements of rules regarding health, safety and wellbeing

    - External Prevention Advisor – SECUREX
      Tel: 02/729.93.18
    - Contrôle du bien-être au travail Direction de Bruxelles-Capitale/Toezicht op het Welzijn op het Werk Directie Brussel-Hoofdstad
      See contact details on https://emploi.belgique.be/fr/propos-du-spf/structure-du-spf/inspection-du-travail-dg-controle-du-bien-etre-au-travail-1#toc_heading_2 (FR) or https://werk.belgie.be/nl/over-de-fod/structuur-van-de-fod/arbeidsinspectie-ad-toezicht-op-het-welzijn-op-het-werk/externe-2 (NL)
    - Police, public prosecutor's office

2. Reports of violation of anti-money laundering provisions

    Cellule de Traitement d'Information Financière (CTIF) – Cel voor Financiële Informatieverwerking (CIF)

    Details are available on the website: https://www.ctif-cfi.be/

3. Reports of violation of data protection provisions

    The Belgian Data Protection Authority

    Information is available on: https://www.dataprotectionauthority.be/citizen/actions/lodge-a-complaint

4. Fraud, corruption, other illegal activities

    Police/judicial authorities (public prosecutor's office)

5. Breach of the Code of Conduct, BIO law, Management Agreement:

    Chairperson of the Audit Committee
    Pieter Verhelst
    pieter.verhelst@boerenbond.be