IBA Anti-Fraud Policy

Act with honesty, never tolerate fraud, follow the controls, spot red flags, speak up without fear of retaliation and cooperate with investigations

Version: v0.1 | **Date:** 15 November 2026 | **Owner:** Legal & Compliance |

Document owner	Chief Legal Officer / Legal & Compliance
Policy sponsor	Chief Legal Officer
Reviewed by	Finance, Internal Audit, Human Resources, Quality, Regulatory Affairs, Information Security and Trade Compliance
Approved by	Executive Management
Effective date	15th November 2026
Review cycle	At least every two years, or earlier if required by law, risk assessment, audit findings or material business changes
MID reference	149 301

1. Purpose and commitment

IBA is committed to conducting its business with integrity, transparency, accountability and respect for the law. Fraud, attempted fraud, corruption, misappropriation, falsification, concealment of material information and any dishonest conduct are incompatible with IBA's values, its Code of Business Conduct and the trust placed in IBA by patients, customers, shareholders, employees, healthcare partners, research institutions, public authorities and other stakeholders. This Policy must be read together with the IBA Code of Business Conduct, including in particular its principles on doing what is right, acting with honesty and integrity, complying with the law, avoiding conflicts of interest, maintaining accurate company records and internal controls, protecting confidential information and intellectual property, data privacy, fair competition, international trade rules, anti-bribery and corruption, reporting concerns and non-retaliation.

This Policy sets out IBA's zero-tolerance approach to fraud and establishes the principles, responsibilities and procedures for preventing, detecting, reporting, investigating and remediating fraud risks across IBA's activities worldwide. Specific aspects of this Policy may be detailed in other Policies such as the Whistleblower Policy or the Private Investigations Policy.

2. Scope

This Policy applies to IBA SA and all entities controlled by IBA, including employees, temporary staff, consultants, agents, distributors, intermediaries, contractors, subcontractors, suppliers and any third party acting for or on behalf of IBA. It applies to all business activities, functions and geographies, including sales, tenders, installation, service, clinical and research collaborations, finance, procurement, logistics, regulatory affairs, quality, IT, human resources and interactions with public or private healthcare institutions.

3. Legal and regulatory framework

This Policy is designed to support compliance with applicable Belgian, European and local laws, including specifically Belgian criminal law on fraud, forgery, computer fraud, abuse of trust, misuse of company assets, corruption, money laundering and corporate criminal liability; applicable rules on whistleblower protection; public procurement and healthcare-sector integrity rules; anti-money laundering and sanctions-related obligations where relevant; EU rules protecting the financial interests of the Union; and any anti-fraud, anti-corruption, tax, customs, export control, healthcare, medical device and public procurement requirements applicable to IBA's business in markets where it operates.

Where local laws impose stricter requirements than this Policy, the stricter requirement must be followed. Where there is uncertainty, employees and business partners must seek guidance from Legal, Compliance or Finance before acting.

Consistent with the hierarchy described in the IBA Code of Business Conduct, applicable local and international laws always take precedence. Once the law has been observed, the Code of Business Conduct is the core reference within IBA's policy framework, followed by global (including specifically this Anti-Fraud Policy) and local policies and procedures. This Policy is intended to operationalize the Code in the specific field of fraud prevention, detection and response.

4. Definition of fraud

For the purposes of this Policy, fraud means any intentional act or omission involving deception, concealment, misrepresentation, falsification, abuse of position or breach of trust intended to obtain an undue economic, commercial, personal or organizational advantage, or to cause a loss, disadvantage or risk to IBA or any third party.

Fraud may include, without limitation, falsifying accounts, invoices, expenses, time records, tenders, quality records, regulatory files or technical documentation; diverting company assets; manipulating procurement or sales processes; misusing confidential information or intellectual property; concealing conflicts of interest; creating fictitious suppliers, customers or transactions; collusion with third parties; bribery, facilitation payments or kickbacks; cyber-enabled fraud; false claims for grants, subsidies or EU-funded programs; customs, tax or social fraud; and any attempt to commit such acts. These examples should be assessed in light of the Code principles on avoiding conflicts of interest, company records and internal controls, protection of information and intellectual property, data privacy, fair competition, international trade rules and anti-bribery and corruption.

5. Guiding principles

- **Zero tolerance:** IBA does not tolerate fraud or attempted fraud, regardless of value, seniority, business pressure or perceived benefit to IBA, consistent with the Code's requirement to do what is right and act with honesty and integrity.
- **Integrity over opportunity:** business objectives must never be achieved through dishonest, misleading or unlawful conduct, including conduct contrary to the Code principles on anti-bribery and corruption, fair competition, public-sector interactions or international trade rules.
- **Accountability:** every employee and business partner is responsible for preventing, detecting and reporting fraud risks, in line with the Code's applicability to IBA employees, consultants and people acting on IBA's behalf.
- **Segregation and transparency:** material decisions, payments, approvals and commitments must be properly documented, reviewed and authorized, consistent with the Code principles on company records and internal controls. No individual should control all critical stages of the process, where segregation is impracticable, independent compensating review is required
- **No retaliation:** people who report concerns in good faith are protected against retaliation, in accordance with the Code's reporting and non-retaliation commitments, applicable Whistleblower Policy and IBA procedures.
- **Fair process:** all reported concerns will be assessed objectively, confidentially and with respect for the rights of the people involved, consistently with the Code's guidance on reporting, confidentiality and responsible escalation.

6. IBA-specific fraud risk areas

Given IBA's specialized activities in proton therapy, radiopharmaceutical solutions, medical technology, service operations and international collaborations, particular attention must be paid to fraud risks in the following areas:

- **Public and hospital tenders:** bid manipulation, collusion, undisclosed intermediaries, false certifications, improper influence or misleading technical representations.
- **Healthcare and research relationships:** improper benefits to healthcare professionals, hospitals, universities, research centers, public officials or patient-related institutions.
- **Large projects and installations:** inflated claims, false milestones, concealed delays, improper change orders, manipulation of acceptance tests or service reports.
- **Regulatory and quality documentation:** falsification or concealment of records relating to medical devices, radiation safety, product quality, clinical use, complaints or corrective actions.
- **Export control and sanctions exposure:** misrepresentation of end users, destinations, beneficial ownership, dual-use risks or restricted-party screening.
- **Procurement and supply chain:** fictitious suppliers, conflicts of interest, kickbacks, inflated pricing, non-transparent subcontracting or false delivery records.
- **Finance and accounting:** improper revenue recognition, false invoices, expense fraud, payment diversion, manipulation of provisions, reserves or project margins.
- **Cyber and information systems:** phishing, business email compromise, invoice redirection, unauthorized access, manipulation of master data or misuse of digital credentials.

- **Intellectual property and confidential information:** theft, unauthorized disclosure, misuse of know-how, software, technical drawings, customer data or trade secrets.

7. Prevention and internal controls

IBA will maintain a risk-based anti-fraud control framework proportionate to the nature, scale and complexity of its activities. This framework must include appropriate due diligence on third parties; segregation of duties; approval thresholds; documented delegations of authority; contract review; competitive procurement processes; accurate books and records; payment controls; master-data controls; inventory and asset controls; project governance; IT access controls; sanctions and export-control screening; and periodic monitoring, testing and audit.

The anti-fraud control framework must support the Code principles on company records and internal controls by ensuring that business decisions, payments, tenders, regulatory submissions, quality records, sustainability information and financial reporting are accurate, complete, traceable and capable of independent verification.

Employees must not bypass controls, split transactions to avoid approval thresholds, create or approve transactions without supporting documentation, approve their own expenses or transactions, use personal bank accounts for business payments, accept or offer improper advantages, or knowingly ignore red flags.

8. Third parties and intermediaries

IBA may be held responsible for misconduct committed by third parties acting for or on its behalf. Agents, distributors, consultants, lobbyists, customs brokers, logistics providers, suppliers and other intermediaries must therefore be selected, approved and monitored in accordance with IBA's due diligence and contracting procedures and the Code principles on anti-bribery and corruption, avoiding conflicts of interest, international trade rules, respect for ethical business conduct and protection of IBA's reputation. Contracts with higher-risk third parties must include appropriate anti-fraud, anti-corruption, audit, termination, sanctions, confidentiality and compliance cooperation clauses.

9. Books, records and financial integrity

All transactions must be accurately, completely and timely recorded in IBA's books and records. No undisclosed or unrecorded account, fund, asset, liability or arrangement may be established or maintained. Supporting documentation must reflect the true nature, purpose, amount and parties to the transaction. False, misleading, incomplete or backdated records are prohibited. This requirement implements the Code principle on company records and internal controls and supports IBA's obligation to maintain reliable financial, sustainability, quality, regulatory and operational information.

10. Reporting concerns

Any employee or third party who becomes aware of suspected fraud, attempted fraud, control circumvention, retaliation or a material red flag must report the concern promptly through one of the available reporting channels identified in the Code of Business Conduct and IBA procedures, including line management, Legal, Compliance, Finance, Human Resources,

Internal Audit or IBA's whistleblowing channel, SpeakUp. Reports may be made in good faith even where the facts are not fully established.

IBA will handle reports in accordance with applicable confidentiality, data protection, labor law and whistleblower protection requirements and consistently with the Code's Speak Up, reporting and non-retaliation commitments. Retaliation against any person who reports a concern in good faith, assists an investigation or refuses to participate in fraud is strictly prohibited. These principles are detailed in IBA's Whistleblower Policy.

11. Investigations and response

Suspected fraud will be assessed promptly and, where appropriate, investigated by people with suitable independence, expertise and authority and in compliance with the Private Investigations Policy. Investigations may involve Legal, Compliance, Finance, Human Resources, Internal Audit, Information Security, external counsel, forensic experts or other specialists, in line with applicable law and company policies. IBA will preserve relevant evidence, maintain appropriate confidentiality, respect legal privilege where applicable and comply with applicable data protection and employment law requirements.

Where fraud is confirmed or reasonably suspected, IBA may take corrective and disciplinary measures, recover losses, terminate contracts, improve controls, notify insurers, auditors, regulators, public authorities or law enforcement where required or appropriate, and cooperate with competent authorities, including Belgian, European or foreign authorities with jurisdiction.

IBA explicitly reserves the right, where relevant, to file criminal law complaints involving alleged or proven fraud incidents, as well as civil lawsuits for damages where such fraud has been proven by a court of justice.

12. Roles and responsibilities

- **Board of Directors and Audit & Risks Committee:** oversee the anti-fraud control environment, significant fraud risks, material incidents and remediation.
- **Executive Management:** set the tone from the top, allocate resources and ensure implementation of this Policy.
- **Legal and Compliance** (in the person of the Chief Legal & Compliance Officer)**:** maintain this Policy, advise on legal requirements, support investigations and monitor compliance risks.
- **Finance:** maintain financial controls, accounting integrity, payment controls and fraud risk monitoring.
- **Internal Audit:** provide independent assurance on the effectiveness of controls and recommend improvements.
- **Managers:** implement controls, address red flags, promote ethical conduct and escalate concerns promptly.
- **Employees and third parties:** act with integrity, comply with controls, keep accurate records and report suspected misconduct.

13. Training, communication and certification

IBA will provide risk-based training and communication on fraud prevention, reporting obligations, red flags and ethical decision-making. Employees in higher-risk functions,

including sales, procurement, project management, finance, regulatory affairs, quality, logistics and management roles, may be required to complete periodic certifications confirming their understanding of and compliance with this Policy and the relevant principles of the IBA Code of Business Conduct, including anti-bribery and corruption, conflicts of interest, company records and internal controls, protection of information and intellectual property, data privacy, fair competition and international trade rules.

14. Breaches and disciplinary measures

Any breach of this Policy may also constitute a breach of the IBA Code of Business Conduct and may result in disciplinary action, up to and including dismissal, termination of business relationships, recovery of losses, civil claims and reporting to competent authorities. Disciplinary measures will be proportionate, consistent and compliant with applicable law.

15. Review and continuous improvement

This Policy will be reviewed periodically and updated when necessary to reflect changes in IBA's business, fraud risk profile, regulatory environment, enforcement trends, internal audit findings, investigation outcomes and lessons learned.

This includes a root cause assessment of confirmed incidents and whether similar exposure exists elsewhere in IBA, with corrective actions followed through to completion.

* * *

Annex 1 — Operational guide: fraud red flag examples

Purpose. Use this guide as a quick operational check before approving, signing, paying, shipping, recognizing revenue, submitting documentation or engaging third parties. A red flag does not prove fraud, but it must be documented and escalated where it cannot be promptly and properly resolved in compliance with this Policy.

Risk area	Typical red flags	Immediate response
Cross-cutting	Pressure to bypass controls; secrecy; altered, backdated or missing documents; unusual urgency; transaction inconsistent with substance; undisclosed personal links; cash/offshore/third-party payments.	Pause where lawful, safe and practicable; document facts and escalate.
Sales, tenders and healthcare interactions	Improper influence; unofficial payments, gifts, travel or sponsorships; customer-, official- or third party-selected intermediary; bid or pricing irregularities; side letters; contacts with competitors on tenders, prices or customers.	Involve Legal/Compliance before committing or submitting.
Third parties and partners	Refusal of due diligence; unclear ownership or role; high commissions; public-official/customer links; adverse media; offshore or unrelated payment requests; end-user/end-use opacity.	Do not onboard, pay, renew or continue the relationship without appropriate clearance.
Procurement and supply chain	Unjustified single source; repeated same supplier; bank-account changes; mismatched PO, invoice, delivery or receipt; supplier links to employees; emergency/manual approvals.	Verify independently and involve Finance/Procurement/Compliance.
Projects, service and acceptance	Milestones or acceptance inconsistent with work performed; pressure to recognize revenue early; unsupported change orders or claims; concealed delays, defects, non-conformities or complaints.	Hold approval/revenue/payment until evidence is verified.
Regulatory, quality and technical records	Incomplete or altered test, validation, complaint or corrective-action records; pressure to omit, minimize or delay adverse information;	Escalate to Quality, Regulatory Affairs, Legal or Compliance.

	uncontrolled files or shadow records.	
Finance, expenses and payments	Vague invoices; duplicate or round amounts; missing support; unusual journal entries, provisions, write-offs or credit notes; excessive expenses; urgent payment override requests.	Do not approve until supporting evidence is complete.
Cyber, data integrity and trade controls	Bank-detail change by email; urgent confidential payment requests; suspicious login or access changes; use of personal tools; unclear end user, end use, route or destination; resistance to screening.	Verify through a trusted channel; involve IT Security for cyber/data issues and Trade Compliance/Legal for export-control, sanctions or customs issues.

When in doubt — stop, preserve, escalate. Operational teams must preserve relevant documents, emails, messages and system records; avoid tipping off people who may be involved; and promptly contact the appropriate manager, Legal, Compliance, Finance, Internal Audit, Information Security, Trade Compliance or the whistleblowing channel. Retaliation against good-faith reporting is prohibited under the IBA Code of Business Conduct.

* * *