Institutional policies

Anti-fraud and anti-corruption policy

Division Risk and Audits Department
Update July 2025

IP ı n°04

Version	Approved by
Initial Version 2007	General Direction
Update Version1° 2011	General Direction
Update Version 2 2019	the Board of Trustees
Update Version 3 2021	the Board of Directors (Directoire).
Update Version 4 2025	the Board of Directors (GEC), Social and Economic Committee (CSE)
Next review 2030	

Contents

1. Fraud and corruption: obstacles to international aid 4

1.1. Defining fraud and corruption 4

1.2 The effects of these phenomena 4

2. HI and the fight against fraud and corruption 5

2.1 Principles 5

2.2 A pragmatic approach 6

1.3 Scope of this policy 7

3. Measures to combat fraud and corruption. 7

3.1 Promoting an anti-fraud and anti-corruption culture 7

3.2 Anticipation, prevention and deterrence 8

3.3 Due diligence and detection 8

3.4 Internal control and internal audit 9

3.5 Reporting suspicions and alerts 9

3.6 Internal investigations and handling of proven cases 9

3.7 Information for third-party organizations 10

3.8 Monitoring and experience learning 10

Focus : the main risks 10

4. Coordination and monitoring 11

4.1. The management commitment 11

4.2. Anticipation, prevention, and deterrence 11

5. Validation and dissemination of this policy 12

6. Glossary 12

1. Fraud and corruption: obstacles to international aid

1.1. Defining fraud and corruption

As part of its mission and activities, HI must protect itself against the risks of misappropriation of its financial and material resources, against fraud and corruption.

1.1.1. Fraud refers to acts which, by deliberately circumventing internal, contractual or legal rules, aim to obtain an undue material or moral advantage, to the detriment of HI or third parties: individuals, communities, organizations, companies or institutions.

1.1.2. For the sake of simplicity, we have grouped together a few different areas and methods of fraud:

- Theft and accounting or financial fraud,
- Logistical fraud, diversion and material theft,
- Human resources fraud and conflict of interest,
- Project and beneficiary fraud, diversion and extortion.
- Data breach

(See details in the glossary on page 12).

1.1.3. Corruption adds the notion of abuse of power. As far as it implies that persons vested with authority, responsibility or delegation will use their position to procure undue advantages of any kind, for themselves or for a third party.

1.1.4. While fraud can be committed unilaterally by an individual or a group of individuals, corruption involves a "transaction" and consideration in the form of money, favours, or advantages. Thus, certain forms of corruption can take the form of soliciting, promising, offering, giving or accepting an undue advantage, in money or in kind. This affects the normal exercise of a function and constitutes a legally or ethically reprehensible act.

1.2 The effects of these phenomena

Fraud and various forms of corruption can be observed in all countries and all sectors of society, and are a constraint on multilateral or bilateral international cooperation, development or humanitarian aid programs.

The fight against fraud and corruption at national and international level is first and foremost

the responsibility of local and international authorities, including international agencies and cooperation donors.
Aware of the risks and stakes for their resources, their image, their interventions and the effectiveness of their actions in favour of beneficiaries, non-governmental organizations must also confront these phenomena at their own level.

2. HI and the fight against fraud and corruption.

2.1 Principles

Preamble

Assuming its responsibilities as a non-governmental actor committed to international action, mindful of the sector's professional ethics, engaged in a constant effort to ensure sound management of its operations and activities, HI takes all measures in its power to prevent risks of loss or misappropriation of the resources entrusted to it.

2.1.1. As such, HI does not tolerate fraud and corruption in the conduct of its activities and implements measures to reduce their risks and effects. The "Zero Tolerance" principle implies that context-specific actions are taken in response to any suspicion or proven incident.

2.1.2. HI adapts its preventive and corrective measures by considering the different categories of harm and levels affected by fraud and corruption, first and foremost:

- Members and staff,
- The beneficiaries of our actions, as far as access to services and assistance is reduced or hindered,
- The partner organisations potentially affected,
- Our organization and the economic balance of our programs.

2.1.3 In the field, in situations of political violence and armed conflict, HI exercises particular vigilance to avoid any risk of instrumentalization or diversion of the resources of its activities for the benefit of military forces or armed groups, whatever their status and motivations.

2.1.4 HI does not tolerate any form of influence peddling in connection with local, national or international public authorities or private entities, whatever the country or activity concerned.

2.1.5 This being the case, HI cannot bear alone the burden and responsibility of fighting corruption in the environment in which it operates. As far as its activities are concerned, HI

acts appropriately within the limits of its prerogatives and resources, giving priority to the individual safety and security of its personnel.

2.1.6 In its commitment to fight fraud and corruption, HI is careful not to encourage a culture of mistrust and generalized suspicion.

2.2 A pragmatic approach

2.2.1. HI adopts a pragmatic approach, based on an analysis that considers: risks specific to each of the countries in which it operates; risks inherent to each function/business line carried out by its personnel; risks associated with each professional sector in its operating context.

2.2.2 Risk monitoring is based on internal tools and mechanisms that enable us to cross-reference data published by specialized organizations (such as Transparency International) with incident reports produced by our own departments (existing tools, as well as those to be developed, are constantly adapted to realities and needs).

2.2.3 Monitoring makes it possible to prioritize actions to prevent fraud and corruption in the countries, with staff and beneficiaries most at risk. The identification of priorities considers the financial and material volumes committed by country, program and activity, as well as the reputational stakes for the organization.

1.2.4 Measures to prevent and combat fraud and corruption[1] concern in particular:

- Staff recruitment and training,
- Project planning, risk assessment,
- Management and internal control,
- Management and handling of known and proven cases,
- As well as collaboration with other organizations in this field.

2.2.5 These measures are monitored and evaluated by the organization's internal bodies, which take the necessary corrective action as quickly as possible and provide support and even protection for people who may be involved in disclosing misconducts.

[1] Anti-fraud and anti-corruption measures may resonate with other policies and provisions, such as the **Protection of Beneficiaries from Sexual Exploitation, Abuse and Harassment**, HI Policy, October 2011, updated 2019, the **HI Code of Conduct** updated in 2021, or **the Prevention of Diversion of Aid to Terrorist Organizations Guidelines**, HI 2024 (restricted distribution).

1.3 Scope of this policy

2.3.1 Members and staff of the organization. This policy and its provisions apply to the following categories with the variations mentioned: permanent members and staff of HI (whatever their status: volunteers, board members, salaried employees or trainees) and more generally to any person or associated or intermediary body, employed by the organization and acting on its behalf.

Consequently, HI ensures that they are informed of the existence of this policy and its implications.

2.3.2 Operational partners (organizations and institutions). HI also takes the measures of information, risk management, support and control that this policy implies, within the framework of relations with operational partners, who although not acting on its behalf, interact with it within the framework of partnership agreements.

2.3.3 Companies and suppliers of goods and services. HI also takes information, risk management and control measures with companies, suppliers and consultants who interact with it under contract.[2]

2.3.4. **Sanctions.** In the event of failure to comply with the provisions of this policy, HI reserves the right to take disciplinary action, terminate contracts, impose penalties, or take legal action against the perpetrators of misconducts.

3. Measures to combat fraud and corruption

The implementation of this policy, through the mobilization of staff and measures to prevent and combat fraud and corruption, is the primary responsibility of managers, both within the various entities of the HI network and in the field.

3.1 Promoting an anti-fraud and anti-corruption culture

3.1.1 HI's bylaws, mission and strategy, institutional policies and directives, management and internal control rules and procedures, reinforced by this anti-fraud and anti-corruption policy, are the main reference points for HI's members and staff.

---

[2] IP 09 Institutional logistics management policy, (internal document), Notably acceptance of the conditions laid down by **HI's Rules of Good Business Practice** reference framework, for any company submitting a bid.

3.1.2 On this basis, our organization is committed to the following initiatives: awareness-raising, training and information campaigns for its members and staff, both at the headquarters of HI network entities and in the field.

3.1.3 As such, our organization makes an ongoing effort to raise awareness among executives and managers to avoid any conflict of interest - actual or potential - between their private interests and the interests of HI.

3.2 Anticipation, prevention and deterrence

3.2.1 As a transparent management and prevention measure, HI managers and staff are asked to draw up an annual declaration of conflicts of interest.

The procedures for drawing up and collecting declarations are set out in: *DI 13 - Conflicts of interest: Guidelines for implementing declarations*.

3.2.2 The organization's managers, at all levels, are responsible for ensuring that opportunities for fraud and corruption are reduced. They have a particular responsibility to identify the nature and level of risk to which our activities and resources are exposed. They also assume their managerial responsibility for internal control.

3.2.3 As part of their duties, they are advised by various support departments with expertise in their fields. As such, they can benefit from analyses (typology of activities or risk zones), advice on the implementation of information, prevention, control and protection measures. This not only reduces the number and severity of incidents but also acts as a deterrent. This, insofar as the existing system is known and provides for the application of sanctions.

3.3 Due diligence and detection

3.3.1 As a precautionary measure, HI performs due diligence on candidates, partner organizations and suppliers with whom it contracts, to assess their legal and reputational status.

3.3.2 These verification and detection measures, which ensure that HI does not enter contracts with persons or entities subject to prosecution or sanctions, are conducted in strict compliance with regulations.

3.4 Internal control and internal audit

3.4.1. Control initiatives measures implemented by managers on the activities they supervise are an integral part of managerial responsibilities relating to internal control. They are decided as part of an internal planning process for each entity or department. These controls enable the detection of wrongdoings, irregularities, and embezzlement (see glossary: Internal control).

3.4.2 Specific directives, guidelines and support materials for awareness-raising, risk management and internal control are drawn up by the relevant departments for each professional area. These documents are available internally from HInside.

3.4.3 In addition, internal audits are decided by the federal governing bodies. They are organized in several ways: as part of an annual audit plan; decided at random; triggered in response to a risk alert or reassessment.

3.4.4 Reports and recommendations are analysed for the benefit of the audited divisions and programs, and more generally for the overall organization. N.B. Internal control (which aims to verify compliance with rules) and internal audit (which seeks to assess the level of risk control) should not be confused with internal investigations (see § 3.6).

3.5 Reporting suspicions and alerts

3.5.1 Members and staff of the organization are invited to report suspicions of fraud and corruption in accordance with the conditions of confidentiality and security set out in the organization's whistleblowing guidelines. These conditions provide for the protection of system users.

3.5.2 Reporting mechanisms are available both internally, for members and staff, and externally, for beneficiaries, partner organizations or suppliers of goods and services.

N.B. See Institutional Guideline *DI 02 - Reporting suspicions of fraud or abuse*.

3.6 Internal investigations and handling of proven cases

3.6.1 Managers are provided with a reference manual containing instructions for conducting investigations. This internal investigation manual is for the use of duly authorized persons only.

3.6.2 The purpose of internal investigations is to verify the existence of breaches or deliberate violations of our internal policies and directives, and where appropriate to establish individual responsibility. The investigation report, which is always confidential, is intended for managers in positions of authority and responsibility. The report's conclusions enable the managers concerned to choose the appropriate measures, including - when misconduct is proven - deciding on the sanctions to be applied or the legal recourse to be taken.

N.B. Internal investigations should never be confused with evaluation, internal control or internal audit activities (see § 3.4).

3.7 Information for third-party organizations

3.7.1 In certain circumstances, determined by legal or contractual provisions, HI may be required to transmit information relating to incidents of fraud, under conditions of security and confidentiality.

3.7.2 These notifications to authorized bodies and donors are governed by a specific HI procedure. They are subject to approval by HI management and comply with regulations on the protection of personal data.

3.8 Monitoring and experience learning

Incidents are recorded and reported, enabling them to be analysed and used not only by the organization's departments concerned, but also by risk management and internal audit bodies.

Focus: the main risks

Operations, techniques and quality:

- Fraud in the context of projects or in relation to beneficiaries (targeted projects and partnerships, misappropriation of aid, misuse of aid, extortion to obtain aid or extortion of beneficiaries, etc.),
- Fraud on performance or results of activities (manipulation of data, indicators, and reports),
- Significant fraud incident involving a partner organization.

HR resources:

- Fraudulent recruitment (favouritism and conflict of interest),

- Payroll fraud or any element of remuneration (fictitious employees, undue bonuses, salaries paid more than once, expenses, compensation based on false receipts, various undue allowances, etc.).

Finance:

- Fraudulent disbursements (excessive or fictitious),
- Bank transfer to a fraudulent account (supplier, partner, employee),
- Cash theft (in offices, during transport, within projects, during bank withdrawals or transfers),
- Exchange rate fraud (unauthorized parallel transactions diverting the difference between an official exchange rate and a free or black-market rate).

Logistic:

- Fraud or collusion in purchasing - Fraudulent selection of suppliers through favouritism or commission taking,
- Fraud or collusion in purchasing - Fraudulent invoicing (over-invoicing, false invoices, misrepresentation of quality, etc.),
- Theft or misappropriation of equipment and materials (including vehicles),
- Abusive use of the organization's resources or equipment for travel (private travel at the organization's expense, road or rail travel, plane tickets, etc.).

4. Coordination and monitoring

To support the commitment of its staff, HI has set up appropriate coordination mechanisms and initiatives, to coordinate the policy and verify its application.

4.1. The management commitment

This policy is coordinated, monitored, assessed, and updated at the highest level of the organization: the Federal General Management and the Executive Board, by delegation from the Global Executive Committee (GEC). The policy and its implementation are supervised by the Board of Directors' Audit Committee.

4.2. Anticipation, prevention, and deterrence

Coordination involves the mobilization of various entities and departments, including:

- coordinating internal control and risk management,
- steering and management of programs and support services,

- coordination and appraisal of various measures to prevent and combat fraud and corruption,
- management of tools for monitoring risks and incidents related to fraud or corruption,
- management of internal reporting and investigation systems,
- measures to support, appropriate and guide staff, enabling them to tackle the challenges of the fight against fraud and corruption within the framework set by the organization,
- procedures for notifying the relevant organizations, institutions, and donors.

5. Validation and dissemination of this policy

This version of the Anti-Fraud and Corruption Policy cancels and replaces the version adopted in 2012 and those revised in 2014 and 2019.

This document is intended for use within HI, within HI network entities, in head office departments and in the field.

It is not made public but may be communicated to organizations and institutions as part of the information and management measures set out in the "Scope of this policy" chapter.

6. Glossary

A

Accounting or financial fraud (and theft): any act intended to obtain unjustified or illegal financial gain, or to deprive the NGO or its stakeholders of financial resources. Financial fraud can include theft of cash, embezzlement, intentional manipulation of accounting documents and financial statements, and money laundering, which consists of illegally concealing the origin of money obtained through illicit activities.

Aid diversion: any act aimed at seizing, stealing, altering, or redirecting aid for the benefit of recipients other than the intended beneficiary group. In a conflict context, internal or external actors can commit misappropriation, for the benefit of government or local authorities, armed forces or groups, or any other similar actor.

C

Case management covers the various stages of incident management: detection, analysis and qualification, establishment of facts, responsibilities and impact, mitigation, and

improvement measures, as well as disciplinary, contractual, and legal sanctions, and notification of donors and authorities where appropriate.

D

Data breach: theft, destruction, loss, alteration, unauthorized disclosure of personal and confidential data. Unauthorized access to such data. Deliberate violation of data protection rules and legislation.

Detection, which is most often conducted during preventive controls, consists of identifying anomalies and irregularities that could reveal incidents or attempted misappropriation.

Deterrence aims to discourage potential perpetrators from committing or participating in embezzlement. To this end, it must be demonstrated that the internal culture, control, and physical environment will drastically limit opportunities for fraud, theft or embezzlement, and that attempts will not be left without consequences.

F

Fraud, embezzlement and extortion on projects and beneficiaries: all acts intended to divert resources from projects and activities to the detriment of the quality and performance of aid, and ultimately of beneficiaries. This can include biased choices of project location or resource allocation, deception in needs assessment or targeting criteria, favouritism in the selection and monitoring of local partners. This can take the form of exclusion or, conversely, the inclusion of ineligible beneficiaries. It can include any manipulation of information to mislead supervisors about the progress of activities, the number and status of beneficiaries, manipulation of registers of acts and services, multiple or "ghost" registrations, false, exaggerated, or incomplete reports. Fraud can also cover the blocking, diversion or extortion of aid delivered, during or after distribution.

H

Human resources fraud: any act intended to obtain an unjustified or illegal advantage to the detriment of the NGO or other employees. This may include fraud in the reimbursement of expenses or health benefits, unauthorised personal use of the organisation's resources, fraud on time sheets, attendance sheets or travel allowances. It may also include the creation of fictitious employee accounts, conflicts of interest, favouritism in recruitment and career development, extortion or taking commission on the salary or allowances of other employees.

I

Internal control: control is an operation designed to determine, using appropriate means and expertise, whether rules have been applied, i.e. whether actions conducted comply with professional requirements and procedures. Control includes verifying the reality, relevance, and proper execution of activities, as well as the reliability of logistical or financial information. It also includes the detection of any irregularities. Findings are the subject of an internal control report, and irregularities which are deliberate violations of the rules are the subject of a report which may lead to an internal administrative investigation.

L

Logistical fraud, embezzlement, and material theft: any act aimed at the theft, misappropriation or unjustified, irregular, or illegal use of premises, vehicles, equipment, goods or services intended for the NGO or its projects. Logistical fraud may include any manipulation of information to falsify the appearance of the situation or the regularity of transactions, false invoices, over-invoicing, disbursement fraud, manipulation of purchase, delivery, and inventory records. It may involve illicit commissions and bribes, facilitation payments, conflicts of interest and favouritism in the selection of suppliers. It also concerns the improper withdrawal of equipment from stock, deception about the quantity and quality of goods and services, including in construction work, and the violation of child labour laws.

M

Material or financial assistance to armed forces or groups: illicit use of the organization's resources to provide material or financial support to armed groups. This includes individuals or groups designated as terrorists by national governments or international authorities.

P

Prevention consists of reducing the likelihood of risks occurring. It is based on procedures that consider the specific risks of misappropriation, due diligence, preventive internal controls, and appropriate corrective measures.

Anti-fraud and anti-corruption policy

This document outlines HI's approach to preventing and fighting fraud, bribery and corruption. It contains a policy framework, objectives and implementation measures.

Humanity & Inclusion
138, avenue des Frères Lumière
69371 Lyon Cedex 08
France
publications@hi.org