DI

Institutional Directive

Whistleblowing Guidance
Reporting suspicions
on fraud and abuses

Risk and Audit Division

September 2025

DI | 02

Version & Date	Validated by
Initial Version - 2007	General Direction
Version 2 – September 2025	Global Executive Committee (GEC) and Social and Economic Committee (CSE)
Next review 2030	

Contents

This Institutional Directive supplements: PI 02 Child Protection Policy, IP 03 Protection of Beneficiaries from Sexual Exploitation, Abuse and Harassment, and IP 04 Anti-fraud and Anti-corruption. Prior reading of this policy is essential to understanding the issues and principles guiding this Directive.

---

1. General framework

1.1. Defining the framework

Our organization has put in place steering, information, administration and control mechanisms that are designed not only to ensure the proper management of our activities, but also to prevent actions that could result in:

- To affect our resources, the integrity of our operations and the quality of the aid provided to the beneficiaries of our projects.
- To harm the physical, mental or moral integrity of the dignity of people, HI employees, beneficiaries and partners, or community members in the countries where we operate.

1.2. Responsibility of directors and managers

These general mechanisms form the basis for specific measures to fight fraud, corruption and abuse. And to ensure that these mechanisms are effective, directors and managers are responsible for informing the organization's members and staff about the key principles of internal control and how we operate. To this end, information and training measures are being taken to raise awareness among members and staff at the head offices of federal network entities and in the field. To ensure that this information is complete, it also specifies the whistleblowing procedures for reporting suspicions and incidents. Transparency in this area can only contribute to a safe working climate, which encourages prevention and the use of available reporting.

2. Reporting procedures accessible to HI members and staff

HI members and staff have a number of options for reporting suspected or discovered acts of fraud, corruption, sexual abuse and exploitation, child abuse and any other abuses against individuals, which must meet the requirements of professionalism, confidentiality and safety for both the individual and the organization.

2.1 Informing management

2.1.1 The first solution is to inform the management chain, which remains the usual priority channel for reporting. The risk and incident management system is currently based on guidelines, handling and reporting procedures that give priority to ordinary case management by line management, with the support of functional or thematic referents.

2.1.2 This usual management method involves a request to the line manager, accompanied by information to the specific specialist (human resources, finance, etc.). Depending on the type of incident encountered, managers in the field and at head office are called in to handle an incident, with the support of the relevant support departments.

2.1.3 The person reporting a suspicion or incident must do so as soon as possible. They are not requested to investigate or compile a file of evidence before making the report. These tasks may only be carried out on explicit instruction by people designated by management.

2.1.4 In formal terms, all incidents involving acts or omissions, whether unintentional or deliberate, generating harm or risk for individuals or the organization, are reported via the available incident media to the levels of responsibility and head office departments best placed to manage suspicions or proven cases.

2.2 The ability to alert higher levels of the organization

2.2.1 However, in certain circumstances, the person who suspects or discovers a case of fraud, corruption or abuse may find it difficult or risky to refer the matter to the next level up. There are several reasons for this:

- fear that the line manager will not be able to manage the report in the association's best interests,
- fear that this supervisor may be involved in the acts under suspicion,
- fear of punishment or more or less well-founded negative consequences.

2.2.2 In practice, a person may bypass one or more levels of the hierarchy to speak to a higher-level manager, either in the field or at head office. For instance, an employee who struggles to speak to their manager could contact the programme director in the field directly, or even the geographical or regional director, or the human resources department at headquarters. This approach is applicable to all levels of the organisation, in both the field and headquarters, and to all departments.

2.2.3 In addition to the managerial and hierarchical channel for reporting information, our organization set up a centralized system (exclusively internal), attached to General Management and the Federal Chairperson, to collect professional alerts.

2.2.4 Reports are received and followed by a cell made up of directors and managers from the International Programs Department or the concerned entities and the Risks and Audits Department (DRA). Since 2020, this system has been supported by a secure whistleblowing and case management platform (EthicsPoint from NAVEX). The alert mechanism is accessible via the intranet platform of HI - HInside or via the Internet HI site to any HI member or employee, within the federal entity, network associations, at headquarters or in the field.

Please note (1): Any manager who receives a report of abuse or fraud through the hierarchical line must enter this report on the EthicsPoint case management platform. This also applies to any employee who receives a report from members of the community, aid beneficiaries or other external stakeholders wishing to alert the organization through an employee (refer chapter 4).

Please note (2): This whistleblowing system does not in any way replace existing channels for dealing with managerial difficulties. The professional alert is reserved for reporting suspicions of the following facts:

A) Abuse against people

- Discrimination based on religion,
- Discrimination based on disability,
- Discrimination based on gender or sexuality,
- Racism and discrimination based on origin or skin colour
- Bullying & humiliation
- Child abuse
- Moral harassment
- Sexual harassment
- Sexual abuse
- Sexual exploitation

B) Fraud and corruption

- Human resources fraud and conflicts of interest
- Logistical fraud, embezzlement and theft
- Fraud, extortion and embezzlement on projects and beneficiaries
- Theft and accounting or financial fraud
- Material or financial assistance to armed forces or groups
- Violation of sensitive data protection rules.

The whistleblowing and case management platform

The platform EthicsPoint aims at making it easier for people to report serious incidents in complete confidentiality; it allows greater responsiveness, through rapid mobilization of top management, who can request the implementation of internal investigation, processing and protection measures.

On a practical level, at reception of the alert, a first automatic acknowledgment of reception is produced with a secure key number allowing further follow up by the reporter. Only 2 automatic primary recipients (a senior manager and a thematic advisor) strictly identified in the system and with no conflicts of interest identified (IA) receive the alert and decide if additional assignments are relevant or not.

The first level of case management is to cross-check the protection conditions for the whistleblower (and the victim/survivor in a case of abuse if the persons are different) and to proceed to an initial analysis to qualify the facts: connection with HI, type of allegation, seriousness, details and value of the factual elements, which may lead, depending on the case:

- on controls by operational and support departments, which retain their internal control responsibilities,
- or on an internal administrative investigation, under the responsibility of the Risk and Audits department, with the aim of confirming the existence of fraud or abuse and establishing individual responsibilities.

See appendix: Flow chart for processing alerts

3. The organization’s commitments

So, whatever channel is used - management line, focal point/referent or whistleblowing mechanism - the organization takes steps to inform and protect members or employees who report suspicions or incidents, and whistleblowers, throughout the process. Indeed, users of the various devices need to be assured of the organization's commitments in terms of confidentiality, professional protection and security.

3.1 Respecting confidentiality

HI encourages the reporters to identify themselves, to ensure better handling of the report by opening up the possibility of requesting further details. In return, the managers receiving the information and those in charge of handling incidents ensure that the identity of individuals is treated confidentially. Confidentiality is both an obligation and a prerequisite for the calm handling of reported cases, whether proven or not, and for the safety of people in sensitive situations. All reports are managed with the same rigor and security in the interest of all stakeholders and participants.

3.2 Respect for contractual and professional commitments

Our organization is committed to ensuring that the author of a report will not suffer any personal, professional or career harm.
Indeed, no sanction can be applied against a person who acts in good faith, whatever the results of the investigation, i.e. even if, in the end, no fraud, no misconduct or abuse is confirmed.
Conversely, people who, in the absence of any suspicion use of this mechanism for the sole purpose of harm, to denounce or spread malicious rumors, can be subject to sanctions

3.3 Security

Case managers will take all necessary measures to ensure the personal safety of whistleblowers so that they are not harmed, intimidated or retaliated against.

See Focus box below: **Protection against reprisals.**

FOCUS. Protection against reprisals

Definition: Retaliation is any adverse action taken against a whistleblower acting in good faith, in response to a report. Reprisals may concern the working environment (hostile climate or intimidation), unjustified sanctions (warning, suspension, dismissal), blocking or calling into question the professional situation or development (slowing down or refusing promotions, salary increases or requests for changes in status). (Non-exhaustive list)

1. Protective measures

As a corollary to the obligation to report any suspicion of unethical, illicit, fraudulent or abusive activity, HI undertakes to protect against reprisals any employee who engages in whistleblowing.

1.1 HI makes its members and staff aware of measures to prevent and protect against reprisals, through the usual internal information and training channels.

1.2 Confidentiality being the first of the protection measures, HI has set up a mechanism for collecting reports and alerts which provides for:

- A protocol for the confidential handling of information and alerts,
- Confidentiality of sources and the identity of the authors of reports
- Protection of data collected on a secure platform accessible only to authorized people.

Systematic verification of the whistleblower's situation at the end of the investigation and during the following 6 months (at least 2 times during the period).

1.3 As such, breaches of confidentiality and the disclosure of sensitive personal information may be subject to disciplinary action or even legal prosecution.

2. Consequences of breach of anti-retaliation provisions.

2.1 Any suspicion or observation of retaliation against a whistleblower must be reported immediately via the most appropriate channel: either the Human Resources Department or the EthicsPoint reporting platform, whose technical configuration prevents access to the content of reports by the people named in the report.

2.2 Reports of retaliation are investigated where appropriate.

2.3 As such, any manager or employee who retaliates against another member of the organization involved in a whistle- blowing or alert process is subject to disciplinary measures, up to and including termination of contract.

2.4 Cases of retaliation or proven attempts at retaliation are reported to the management and supervisory bodies.

NB. Anti-retaliation provisions cannot be invoked by employees sanctioned for knowingly making false allegations, deliberately providing misleading information with the intention of harming or obstructing an internal investigation. Similarly, they may not be invoked by perpetrators of breaches or violations of corporate policies or guidelines, or of the Code of Conduct, for the sole purpose of evading sanctions.

3.4 Reviewing information and processing cases

Managers and supervisors receiving reports and in charge of handling incidents undertake to examine all reports promptly. They undertake to keep the authors of the reports informed of the progress of the case, within the limits of what concerns them personally, and of the responses given and any accompanying measures that may be decided[1].

At the end of the process, the results of the checks or investigations should make it possible, depending on the case, either to close the file without further action, or:

- impose any sanctions,
- implement the necessary protection and support measures for the employees, partners or beneficiaries exposed or affected.
- take corrective measures to protect the association's economic, legal and ethical interests.

4. Reporting systems open to external

In addition to internal mechanisms, aimed at the organization's members and staff, other whistleblowing channels are open and accessible for the outside. Aligned with the accountability principles, complaints and feedback mechanisms, systems for communities

[1] That being said, whistleblowers cannot under any circumstances demand access to the case file or confidential information. Furthermore, no information on the progress of a case may be disclosed to whistleblowers or anonymous informants.

and beneficiaries benefitting from our aid and for partners are mandatory deployed in every field project.

4.1 For the beneficiaries of our actions

For all its missions, HI requires the implementation of information, awareness-raising, consultation and feedback mechanisms and initiatives aimed at the beneficiaries of our projects. The aim is not only to accompany the progress of activities, but also to collect opinions, suggestions, contributions, questions, even concerns or grievances.

In addition, although not part of our organization, information from community initiatives (village committees, refugee committees, user committees, beneficiary committees) can enrich our risk analysis and draw our attention to potential incidents.

4.1.1 In situations of high exposure to the risks of fraud or abuse (unstable situation, scale of resources committed, high vulnerability of particularly exposed categories: women, children, etc., scale of human trafficking, obstacles to monitoring of activity), which could affect both beneficiaries and our organization, directors and those responsible for running operations must put in place specific initiatives of information, prevention and complaint gathering. These measures must be planned and budgeted for.

4.1.2 In all cases, beneficiaries need to be informed of two points:

- Conditions for aid (e.g. eligibility criteria, nature or volume of aid, specific terms and conditions for granting aid, non-conditionality, free services, non-discrimination, etc.).
- The possibility of reporting any breach, hindrance or abuse to the organization, while respecting confidentiality.

4.1.3 These systems need to be adapted (form and scope), accessible (proximity, language, without significant cost to users) and consider cultural and technological constraints. HI managers can envisage a number of different solutions:

- **Relational mechanisms**: a person identified as the focal point, reception areas, community meetings, focus groups, individual interviews or surveys, etc.
- **Materials**: posters, audio or radio announcements, suggestion or complaint boxes, dedicated e-mail addresses, telephone numbers, social network accounts, etc.

4.2 For partner organizations and supplies

4.2.1 In the context of contractual relations, partner organizations and companies supplying goods or services must also be informed of the existence of our policies, the people to contact and the means to report and settle any incident or dispute.

4.2.2 Consequently, all contractual documents (partnership agreements, MoU, purchases conditions, service contractors/suppliers contracts) include reference to our policies, a contextualized reporting channel and the link to EthicsPoint platform.

4.3 For institutional and private donors

For donors, the main channel for reports, claims or complaints remains contact with the departments and services in charge of donor relations at federal level or in HI's national associations. However, donors who have witnessed or been the victim of wrongdoing or fraud involving HI's reputation can also use the EthicsPoint mechanism.

DI

Reporting suspicions of fraud or abuse

As an international solidarity organisation committed to respecting the dignity and fundamental rights of people with disabilities and the most vulnerable populations, HI is committed not only to ensuring the protection of its beneficiaries, but also that of all those who come into contact with its activities.

This directive sets out the general framework for collecting and processing reports of suspection of fraud and abuses. As such, it incorporates measures to protect whistleblowers and describes the professional alert mechanism.

Handicap International – Humanity & Inclusion
69371 Lyon Cedex 08
France
www.hi.org