Reporting suspicions on fraud and abuse

Federal Executive Director's Office
June 2018
(actualises and replaces the reporting referential published in 2015)
Institutional directive

Reporting suspicions on fraud and abuse

1. GENERAL FRAMEWORK
   1.1 Defining the framework
   1.2 Actions under the responsibility of directors and managers

2. REPORTING METHODS AVAILABLE TO HI MEMBERS AND STAFF
   2.1 Informing line management
   2.2 The option of alerting more senior levels within the organisation

3. THE ORGANISATION’S UNDERTAKINGS
   3.1 Maintaining confidentiality
   3.2 Abiding by contractual and professional undertakings
   3.3 Safety
   3.4 Examining information and dealing with cases

4. REPORTING MECHANISMS AVAILABLE TO THE OUTSIDE WORLD
   4.1. For the beneficiaries of our actions
   4.2. For partner organisations and suppliers
1. General framework

1.1 Defining the framework

Our organisation has put into place steering, reporting, administration and control mechanisms which are intended to ensure not only the proper management of our activities, but also to prevent scheming, whose effect would be:
- to affect our resources, the integrity of our operations or the quality of the aid intended for our project beneficiaries;
- to cause harm to the physical and psychological integrity and dignity of persons, including HI’s staff, beneficiaries and partners or members of the community in the countries in which we work.

1.2 Actions under the responsibility of directors and managers

These general mechanisms serve as the basis for specific anti-fraud, bribery, corruption and abuse measures. In order to ensure that these mechanisms are effective, the organisation’s directors and managers have a responsibility to inform its members and staff of the key principles underlying internal control\(^1\) over our operations. To this end, measures involving training and the provision of information are being taken to raise the awareness of members and staff at Head Office, in the entities which make up the federal network, and in the field. In order to ensure this information is as comprehensive as possible, it sets out the various ways in which suspicions and incidents, are to be reported. Transparency in this area can only contribute to a harmonious working environment, thereby bolstering prevention and encouraging the use of the available reporting mechanisms.

---

2. Reporting methods available to HI members and staff

Several solutions are available to HI members and staff who wish to report a suspicion or the detection of acts of fraud, bribery, acts of corruption or abuse against persons. These solutions must satisfy certain conditions in terms of professionalism, confidentiality and safety, both for the persons concerned and for the organisation.

2.1 Informing line management

The first solution involves informing the managerial chain, which remains the normal channel and the first choice for reporting suspicions and incidents.

2.1.1 The risk management and incident processing system currently in place is based on guidelines and procedures for reporting and handling incidents, which emphasise ordinary management of cases via the managerial chain, with support from functional advisers.

2.1.2 This normal method of management involves the employee referring the matter to their line manager, and at the same time informing advisers in the specific areas concerned (human resources, finance, etc.). Depending on the type of incident encountered, managers on the field and at Head Office are requested to handle the incident, with the backing of the support services whose Area of responsibility covers the area concerned. For example, in the field, a logistics officer will report a logistics incident to his line management: the support services coordinator, as well as to the Head Office logistics adviser.

2.1.3 A person reporting a suspicion or incident should do so as soon as possible. They are not responsible for conducting an investigation or producing a dossier of evidence. In the case of suspected abuse, the incident will be reported to the field programme director or to the person appointed to fulfill protection functions, as well as the human resources advisor at the Head Office.

2.1.4 Consequently, at a formal level, all incidents involving acts or omissions, whether involuntary or intentional, which give rise to a loss or a risk for persons or for the organisation, are to be reported, by means of the incident reporting forms available, to the hierarchical levels and Head Office units best placed to manage any suspected or proven cases.
2.2

The option of alerting more senior levels within the organisation

2.2.1 Nevertheless, in certain circumstances, a person who suspects or discovers a case of fraud, bribery or abuse may consider it problematic or risky to report the matter to their line management. There may be several reasons for this:
- fear that the line manager in question will be unable to manage the matter reported in the association’s best interests,
- fear that the line manager in question is personally implicated in the acts arousing suspicion,
- a fear of suffering disciplinary action or negative consequences, which may be more or less justified.

2.2.2 In this case, the person wishing to report the incident may approach a more senior level within the structure. In concrete terms, they are entitled to move up one or more levels of the hierarchy in order to contact a manager at a more senior level within the line management structure, either in the field or at Head Office. To take the previous examples (2.1.2), a logistics officer who considers it problematic to approach his direct line manager (the coordinator) will then directly alert the field programme director / head of mission, or even the Head Office programme desk officer or director. In the event of abuse, the person concerned can contact the national or regional director directly, or the Head of the Human Resources Division at the Head Office. Needless to say, this logic applies to the various levels of the organisation, both in the field and at Head Office, and may concern any division.
A centralised whistle-blowing mechanism

In addition to the channel already in place, HI has put in place in 2016 a centralised whistle-blowing mechanism for internal use only reporting directly to the Executive Director and the Federal Chairperson. The receipt and follow-up of reports is ensured by a team made-up of directors and human resources advisors, the Federal Secretariat and the Direction of Operations Division.

This mechanism will ensure:

- That the person reporting a serious incident does not shoulder the entire responsibility for informing the line management throughout the organisation,
- Improved response times, by rapidly mobilising senior management who can request the implementation of verification, processing and reporting measures to address the incident.

This whistle-blowing mechanism is available to all members or employees of HI in the Federation, the national associations, at Head Office, and in the field, on HIinside, HI’s internal information platform.

Before accessing the whistle-blowing form, users of the mechanism will be reminded:

- Of the usual chain for reporting incidents and suspicions (managerial chain, risk and incident management procedures);
- The fact that the whistle-blowing mechanism should only be used in exceptional circumstances. Indeed, the whistle-blowing mechanism should not under any circumstances be regarded as a substitute for the existing routes of recourse and dealing with concerns. It should be activated in the event of a problem along the managerial chain, for serious reasons that might have a significant effect on the organisation;
- The aims being pursued and the areas concerned, the ways in which reporting is to be implemented;

2. As with the traditional method of reporting concerns, via the managerial route, the person who raises the alert is not responsible for conducting the investigation.

3. https://hinside.hi.org/intranet/
The limitations of the mechanism in place, any disciplinary action that will be taken in the event of abusive use;

And conversely, the guarantees given to bona fide users.

On a practical level, the information reported will be acted on in the following stages:

- An initial analysis to assess the facts: seriousness, details and value of the factual information;

- A full investigation that may result, depending on the case:
  - In a managerial control performed by the Division concerned, which will retain its responsibility for internal control;
  - Or an internal audit decided by the Risk Management Committee (Directorate) or the Audit Committee of the Board of Trustees, as appropriate.

This internal whistle-blowing mechanism has been presented to HI's staff representative bodies which have approved its implementation. Furthermore, it complies with the legal and professional requirements imposed by the regulations of the countries in which the head offices are based. Any information provided in order to process the reported incident will be treated in compliance with the French Data Protection Act of 6 January 1978.

For this reason, conforming to regulation, HI does not encourage anonymity, but commits itself to respect strict confidentiality on the identity of people (author of the report, people affected or involved).

Nota bene. This centralised mechanism complements the proximity mechanisms and measures implemented in the field. It does not intend on replacing them.
3. The organisation’s undertakings

Consequently, regardless of the channel adopted – line management or the whistle-blowing focal point - the organisation will take measures to inform and protect any members or employees who report suspicions or incidents, and whistle-blowers, throughout the process.

Indeed, users of the various mechanisms must be assured of the undertakings given by the organisation in terms of confidentiality, protection at work and safety.

3.1 Maintaining confidentiality

HI encourages those who report concerns (or whistle-blowers) to identify themselves, so that the matter reported can be dealt with more effectively, by enabling the organisation to ask for further information if need be. In return, the managers to whom such information is reported, and those responsible for dealing with incidents, must ensure that the identity of those involved remains confidential.

Indeed, confidentiality is both an obligation and a pre-condition for the proper handling of any cases reported, whether proven or not, and for the safety of the persons involved, in sensitive contexts. All of the information reported must be processed with the same degree of rigour and the same regard for safety. Such confidentiality also guarantees the presumption of innocence for those implicated, until such time as the truth of the facts is established via an internal investigation, as well as ensuring professional and harmonious management of any proven cases.

3.2 Abiding by contractual and professional undertakings

Our organisation is committed to ensuring that anyone who reports a matter of concern should not be worried, in a personal capacity, either about their job or their career. In point of fact, no disciplinary action can be taken against anyone acting in good faith, regardless of the outcome of the investigation, i.e. Even if no incident of fraud or abuse is confirmed.

Conversely, disciplinary action may be taken against anyone who,
in the absence of any legitimate suspicions, uses this mechanism abusively in order to harm or denounce others or to start malicious rumours.

3.3 Safety

The managers responsible for dealing with these cases will take all necessary measures to ensure the personal safety of those who report matters of concern, to ensure that their interests are not damaged in any way and that they do not suffer any intimidation or reprisals.

3.4 Examining information and dealing with cases

3.4.1 The managers responsible for dealing with incidents³ (or the whistle-blowing focal point) will ensure that they look into all matters of concern reported to them, without delay.

3.4.2 They undertake to keep those who have reported matters of concern informed regarding the progress of the case, to the extent that such persons are concerned personally, the responses implemented plus any support measures decided upon.

3.4.3 At the end of the process, the outcome of the control or audit should enable one of the following two steps to be taken. Depending on the case, the results of verifications should either lead to the file being closed with no further action to be taken, or to:
- disciplinary measures,
- the implementation of any necessary safeguarding and support measures for HI’s employees, partners and beneficiaries,
- corrective measures to protect HI’s economic, legal or deontological interests.

3. In addition to this document, a specific kit of information, including a flowchart, is made available to managers in charge of prevention measures and processing incidents. This kit, which is updated regularly, is accessible to managers on a reserved space on HINSIDE.
4. Reporting mechanisms available to the outside world

To supplement these internal mechanisms, which are intended for the organisation’s own members and staff, other mechanisms may be created and opened up to the outside world. In particular, this applies in our fields of intervention, where the feedback of information from our project beneficiaries or from our partners is already encouraged, in order to help evaluate the effects of the action taken and to improve our services.

4.1 For the beneficiaries of our actions

4.1.1 HI advocates, for all its missions, that mechanisms and initiatives aimed at the beneficiaries of our projects be put in place to provide information, raise awareness, offer consultation and gather feedback. The aim is not only to announce and accompany these activities as they unfold, but also to gather opinions, suggestions, contributions, questions, and also any concerns or complaints. Furthermore, although this is beyond our organisation’s remit, information derived from community initiatives (committees representing villagers, refugees, users, beneficiaries, etc.), may enrich our risk analysis and draw our attention to any incidents.

4.1.2 Moreover, in situations where there is a high degree of exposure to risks of fraud, bribery or abuse (unstable situation, scale of the resources committed, great vulnerability of particularly exposed categories: women, children, etc., importance of human traffic, obstacles to monitoring the activity), which might affect both the beneficiaries and our own organisation, Directors and Heads of operations must put in place specific initiatives aimed at providing information, ensuring prevention and gathering complaints. These measures must be planned and have their own budget.

4.1.3 In all cases, this involves providing the beneficiaries with information covering two points:

- the conditions governing delivery of the aid (e.g. eligibility criteria, nature or volume of the aid, concrete methods of delivery, non-conditionality, e.g. services provided free, non-discrimination, etc.) ;
- the fact that they can report to the organisation any breaches of procedure, or any obstacles or abuse, while maintaining confidentiality.

4.1.4 These mechanisms must be appropriate (form and scale), accessible (proximity, language, low cost of use) and take into account cultural and technological constraints. Various solutions may be envisaged by HI managers:

- **Relational mechanisms:** having an identified person as a focal point, reception areas, community meetings, focus groups, one-to-one interviews, surveys, etc.
- **Material mechanisms:** posters, audio or radio advertisements, suggestions or complaints boxes, setting up dedicated email addresses, telephone numbers, or social network accounts.

In support to these measures, a centralised e-mail system for the receipt and handling of external complaints is made available to missions in each country. This system’s goal is to ease reactivity of managers in the field, supervision by their regional executive office and a secure preservation by the Head Office.

### 4.2

**For partner organisations and suppliers**

4.2.1 Within the framework of contractual relationships, partner organisations and contractors who supply goods and services must also be informed of the existence of our policies, the persons to be contacted and the methods to be used for reporting and resolving any incidents or disputes.

4.2.2 The safest way to provide this information is to refer to our policies and to mention the possibilities of recourse in contractual documentation.
A centralised system for the receipt and handling of external complaints

In addition to channels for the forwarding of information, HI has put a system in place in 2016 to centralise the receipt and handling of external complaints. A complaints form is available on HI’s website: https://hi.org/en/complaint-process-form

Users are informed that HI, its representatives and staff endeavour to conduct their activity with the utmost professionalism, but that any failings or major difficulties experienced with its programmes or services should be reported to it and will be handled in the strictest confidence.

The complaint form covers the following grounds for complaint:
- organisational problems,
- problems concerning the quality of services or activities,
- misconduct or abuse of persons or abuse of persons,
- acts of bribery or corruption

External complaints are handled by the same team that manages the internal whistleblowing mechanism, i.e. the Human Resources Director, General Secretary and Operations Director.

In conformity with the regulations in force, HI does not encourage anonymity, but undertakes to maintain strict confidentiality with regard to the identity of anyone reporting an incident or making a complaint and those persons affected by it or involved in it.

NB: This centralised mechanism can be supplemented by additional communication tools (social network account). It operates in conjunction with mechanisms and measures in place on the field. It does not replace them.
Contact:
Federal Executive Director’s Office
Reporting suspicions on fraud and abuse

This document is intended to support the implementation of Humanity & Inclusion’s institutional policies and guidelines, especially:

- Preventing bribery and corruption,
- Protecting beneficiaries from sexual exploitation and abuse,
- Code of conduct: preventing abuse and safeguarding persons,
- Child protection.

It presents recommendations for the implementation of the following:

- Internal signaling of suspicions and incidents,
- Reporting in the processing settings,
- Feedback from partners and beneficiaries,
- Whistleblowing.