IP

Institutional Policy

Humanity & Inclusion's Safety and Security Policy

Operations Division
2012 – 2018 updated version

IP I 05

IP

Institutional Policy

Humanity & Inclusion's Safety and Security Policy

1.

Acknowledgments

This document sets forth the safety [1] and security [2] policy adopted by Humanity & Inclusion (HI) for application on its programmes wherever its intervention may be required.

Countries and areas of intervention may present a variety of **specific threats**, including armed conflicts, unstable political or economic environments, weak law enforcement and high criminality rates, religious extremism, natural disasters, health epidemics, poor roads and dangerous driving practices.

HI's legislative and executive bodies, as well as each member of staff involved in field operations, acknowledge to be fully aware of the existence of such risks.

Consequently, HI has made the safety and security of its staff potentially exposed to risk a **priority**, investing ongoing efforts and resources to reduce their exposure.

The **effective protection** of crisis-affected populations is also a major concern for HI. To this end, and to the greatest extent possible, HI endeavours to:

- Ensure access for the populations to impartial and non-discriminatory assistance;
- Avoid exposing people to further risk as a result of its actions;
- Protect people from the physical and psychological harm caused by violence and coercion;
- Help people to assert their rights and recover from the effects of abuse.

To improve its programmes and its access to populations, HI fosters **dialogue with all the relevant actors** in the intervention areas, while ensuring that these relations do not compromise the organisation's independence and impartiality. Modalities of communication are adapted according to the actors and the context.

It is important not to lose sight of the fact that the primary responsibility for protection lies with the states, which have a legal obligation to protect all persons within their territory in accordance with the standards set forth in national law, international humanitarian law (IHL), and refugee law.

Therefore, this policy does not relieve the local authorities of their responsibility either for protecting the populations in the territories under their control or for

3

1. Safety: 'Accidents' caused by nature (e.g., avalanche) or non-violent circumstances (e.g. fire, road accidents) and by illness, injury and death resulting from medical conditions not brought about by violence, or due to lax safety guidelines and procedures in the workplace. *Operational Security Management in Violent Environments, ODI 2010*

2. Security: used here to indicate the protection of aid personnel and aid agency assets from violence, *ODI 2000*

ensuring the safety of the aid workers and organisations assisting these populations.

Neither does this policy relieve governments of their responsibility towards their own citizens when they encounter security problems during their assignment.

2.
Principles

2.1

The **aim of safety and security** management within HI is to enable the implementation of its programmes, while minimising the risks for its staff, partners and beneficiaries.

2.2

Rather than risk aversion, HI's approach to safety and security is **one of risk management**. The organisation endeavours to ensure that it has a sound understanding of its working environment at all times and effective safety and security management procedures in place. The aim is to reduce the risks faced, and to be in possession of the information needed to decide whether the residual risk is acceptable and manageable.

2.3

Rather than deterrence, HI favours **"acceptance"** and **"protection"** in its approach to safety and security management.

2.3.1
"Acceptance" consists in reducing threats by gaining broad consent to HI's presence and actions in the areas in which it operates. Since HI works primarily at community and services level, i.e. alongside the populations, groups of persons and individuals in need of assistance, fostering mutual understanding and acceptance is of paramount importance. In order to achieve this, HI's staff shall respect the existing laws and cultural norms in the area of intervention. All staff shall also promote understanding of the organisation's mission and principles of intervention [3], and conform to HI's ethical standards.

2.3.2
HI's "acceptance" approach must be accompanied by a **"protection"** approach. The "protection" approach focuses on the reduction of staff

---

3. See: HI Scope of Activity and Principles of intervention.

vulnerability through paying close attention to the application of operating procedures and, as appropriate, the use of protective devices [4].

2.3.3

When the combination of the two above-mentioned approaches is not considered sufficient, HI will decide whether recourse to a **"deterrence"** [5] approach is required. In any case, recourse to means of deterrence will always be a last resort and cannot be decided by or imposed on the organisation by any other body than HI's executive. Before this kind of measure is introduced, internal decision-making mechanisms will first take into consideration HI's mandate, principles of intervention and the pertinence of maintaining its activities in a seriously deteriorated environment.

2.3.4

In no circumstances, and in keeping with humanitarian principles, will HI authorise any of its staff to carry a weapon.

2.4

The **operational decisions** taken by HI **take safety and security risks into account at all stages of intervention**, from the design phase through to the withdrawal phase.

2.5

HI defines the **threshold of acceptable risk** in each country of intervention on the basis of **an up-to-date residual risk analysis** [6] provided by the programmes' line management. This risk analysis helps maintain an on-going balance between the principle of solidarity and that of responsibility; i.e. the balance between the benefits for the population aided and HI's obligation to reduce, as far as possible, identifiable risks for its personnel, beneficiaries and partners.

When defining the acceptable level of risk, HI will at least take into consideration:

- Its ability to implement the actions planned
- Possible measures for reducing HI's vulnerability, i.e. reducing the probability of an incident and its

---

4. This can include communications equipment, reliable vehicles, tactical use or non-use of the logo, protection for the premises, etc.

5. A deterrence approach reduces the risk by containing or deterring the threat with counter-threat, e.g. suspension or withdrawal of activities, use of armed escorts or guards.

6. A residual risk analysis is carried out systematically. The residual risk is the result of a combined analysis of threats in the area of intervention (probability and impact), HI's vulnerabilities and the impact of acceptance and protection measures to reduce the risks.

eventual impact.

- Its capacity to cope with the occurrence of an incident, and the impact of such an incident on the continuation of activities.
- The capacity of its implementing partners to manage the risks.

Management, whether at head office or in the field, is responsible for ensuring that its staff understands and is willing to accept the level of risk that they might face.

The risk analysis will also take into account the varying degrees of vulnerability and exposure to risk of its staff on the basis of personal criteria such as gender and nationality and in full conformity with confidentiality requirements.

2.6

Where safety and security conditions deteriorate significantly, management must reassess the risk and make sure that staff are aware of the new level of risk.

2.7

When risk reduction measures are seen to be inadequate and the residual risk deemed unacceptable, HI will withdraw from the area and possibly from the country.

2.8

HI provides its teams with the **procedures and tools they need for managing safety and security**. HI's standards should cover the management of day-to-day safety and security, as well as exceptional crisis management.

2.9

Each HI programme has an **up-to-date set of safety and security procedures, including clearly-identified contingency measures**. These contingency measures will be communicated on a need-to-know basis to those staff responsible for their implementation.

2.10

In some areas, the organisation may decide to restrict rights to privacy and the freedom of movement of its international or delocalised national employees outside working hours in accordance with the level of risk.

2.11

Effective safety and security management requires involvement and discipline on the part of all staff.

Therefore, each member is responsible for:

- **Taking care** of their own safety and

security, i.e. being aware of existing risks and avoiding complacency or putting themselves at unnecessary risk.

- **Contributing** to their own safety and security by complying with by all existing policies and procedures.
- **Participating** actively in the development and maintenance of safety and security measures, and ensuring they are complied with by the staff they manage.
- **Sharing** with their line management any information, observations and perceptions relevant to safety and security.
- **Reporting** actions and behaviour that jeopardize team safety and security, and any incidents occurring.
- **Developing** a respectful approach to the local population and behaving with modesty and discretion at all times.

2.12

If, despite the safety and security approach deployed by HI, **anyone considers her/himself to be in danger, she/he can decide to withdraw from an unstable location**, and stop working in a country or area that she/he considers to be too dangerous. The person should inform her/his manager of the situation without delay to avoid endangering the safety and security of others and so that the evacuation can be organised in the safest conditions possible.

2.13

HI's **partners** are responsible for setting their own safety and security standards out of due respect for the principle of self-determination. Nevertheless, HI needs to ensure that their managers are clear about their role and responsibilities regarding safety and security management. To this end, these aspects should be outlined in the partnership agreement signed by all the parties.

3.
Entry into force

This document was approved by the federal Board of Trustees on June 23rd, 2012[7] and therefore comes into immediate effect. It forms an integral part of the organisation's reference documentation.

This policy applies to:

- **International staff** for the entire duration of their contract and for the entire period (weekends and leave periods included) spent in the country of assignment.
- **National staff** during working hours.
- **Delocalised national** staff for the entire duration of their contract and for the whole time (weekends, leave

---

7. The changes made to this 2018 version mainly concern HI's visual identity.

periods, and any other non-working periods included) spent in the country of intervention until the moment they return to their base.

- **All HI Network (Federation, National associations, HI Institute for Humanitarian Action) staff, volunteers, and Board or General Assembly members** on a field visit from the moment they enter the country of intervention.
- **Consultancy services** contracted by HI as defined in the specific clauses of their contract.

All HI staff and consultants are informed of this policy and their obligations with regard to it when signing their contract.

When joining HI, HI Network staff, international employees, international consultants and delocalised national staff acknowledge and accept that the level of exposure to risk in HI's areas of intervention may be higher than in their home country.

Non-compliance with HI safety and security standards may increase the exposure of staff to risk or cause harm to HI's assets and image. Therefore, failure to comply with this policy, including failure to report breaches of this policy and associated rules, may result in disciplinary action, including dismissal or termination of a contract.

4.
Monitoring

Policy implementation and safety and security practices are monitored permanently at country level by the Field Programme Director (or Head of Mission) and his/her managerial chain at head office.

They are assisted by a Safety and Security Unit, which sets safety and security management frameworks, defines the tools deriving from this policy, and issues recommendations to the managerial chain.

5.
Evaluation

To ensure the continuing relevancy of this policy, it may be amended to take account of lessons learnt from experience.

On any matters concerning the implementation of this policy, please contact: security@hi.org

This policy is supplemented by
a practical guide & a toolbox.

All these elements are available from
our internal HInside platform.

IP

**Humanity & Inclusion's
Safety and Security Policy**

This paper presents Humanity
& Inclusion's policy on security
for all the countries and
settings in which it works.