



# Safety and Security Policy for International Activities

Date : July 2012  
Author : Andre Oostrom, Centre for Safety and Development  
Yearly review : Oktober 2013  
Reviewed by : Andre Oostrom, CSD  
Next yearly review :  
To be reviewed by :

## Content

1. Introduction	1
2. Purpose, Scope and Compliance	2
2.1 Purpose	2
2.2 Scope	2
2.3 Compliance	5
3. Principles	5
4. Responsibilities	5
4.1 Organisation	6
4.2 Board of Directors	6
4.3 Operations Director	6
4.4 Secretariat Board of Directors	7
4.5 Management Team	7
4.6 Staff Members	7
4.7 PSC and HACA	8
5. Security Management Tools	8
5.1 Security Levels	8
5.2 Security Protocols	8
5.3 Security Officer	9
5.4 Crisis Management Team	9
6. Annex	9
6.1 Annex 1: Code of Conduct	10
6.2 Annex 2: Safety and Security Declaration	11

## 1. Introduction

Red een Kind is a Dutch Christian organisation that focuses on support and development of children and youth in Africa and Asia. Red een Kind works closely together with local partner organisations and is active in Southern and Eastern Africa, as well as in India, China, Thailand and other parts of South East Asia.

Since 1968 Red een Kind takes care of disadvantaged and vulnerable children in Africa and Asia. They work to brighten future perspectives for youth who would otherwise barely survive. They are confronted with severe poverty, combined with the terrible consequences of AIDS, hunger, child labour, and violence. Red een Kind provides education, vocational training, and medical care. Additionally they also consider the psychological, social and mental development of the child. Enhancing the capacities of children and youth to sustain themselves is the main goal of Red een Kind, enabling these young people to secure a better future for themselves.

Red een Kind performs its work in countries increasingly affected by insecurity. In addition, there has been a noticeable erosion of respect and understanding of the role of internationally operating not-for-profit organisations, resulting in an increased targeting of aid workers over the past years.

Safety and security is of the highest priority and an integral part of the organisation's duty of care to its staff. This Security Policy document sets the basis for the organisation's position on how it acknowledges and should manage any security risk with the aim to reduce the effects they may have on the organisation, its staff, reputation and assets. It must be clearly noted that although this document outlines Red een Kind's policy on how to mitigate risks, there will always be residual risk; risks cannot be avoided completely.

## **2. Purpose, Scope and Compliance**

### *2.1 Purpose*

The Safety and Security Policy describes the organisation's approach to safety and security and sets out general rules for security management. It has the intention to inform Red een Kind staff members in order to take an active role in reducing risks.

Red een Kind acknowledges that working in certain areas around the world comes with risks towards staff and programmes. Although Red een Kind will do its utmost best to minimise those risks, a certain level of risk will remain while implementing our mission. Red een Kind will strive to ensure that staff is aware of the risks that are involved in their work.

Rather than seeing security management as a restrictive necessity, Red een Kind sees security management as a way of enabling their work and programmes and thus the continuation of operations under conditions where without security management this might no longer be possible.

As a result of the aforementioned considerations, Red een Kind considers security management as a way to:

- Enable operational activities under difficult security conditions
- Reduce the risk to individual staff members to an acceptable level
- Protect the reputation of Red een Kind

The balance between these objectives is carefully decided upon at every level in the organisation and this document will provide clarity on which decisions are made at which level. Every staff member; regardless of his/her function, has the right and duty to contribute to these objectives.

This Security Policy is the main tool in the implementation of security management within Red een Kind and it strives to do so by:

- Outlining clear decision lines and responsibility levels
- Providing guidance in specific security situations
- Ensuring adequate awareness and preparation on all organisational levels

### *2.2 Scope*

The Security Policy applies to all Red een Kind staff; regional representatives, consultants, family members duly authorised to accompany or visit staff during missions, authorised visitors, volunteers in the field, interns and any other person working formally and directly with Red een Kind unless explicitly agreed upon otherwise.

This Security Policy does not include the safety and security of partner organisations. Red een Kind does not bear responsibility for security practices of its partner organizations, regardless of Red een Kind acting as donor to this local partner or not. However, Red een Kind sees it as its moral obligation to support their local partners with their safety and security in the field.

Primarily, Red een Kind bears responsibility for the security of their own employees as a matter of duty of care in the execution of the day to day activities. This includes consultants and other persons not employed by Red een Kind that are working on behalf of Red een Kind in the exercise of the daily activities of Red een Kind; the specific arrangements for which are laid down in the agreement Red een Kind has concluded with these persons.

However, it is not uncommon that Red een Kind staff is joined by others, such as but not limited to journalists, politicians, donors, volunteers and fundraisers. The behaviour of these others might affect the security of Red een Kind staff. Although the (contractual) relationship between these others and Red een Kind is different from the relationship with its own employees, Red een Kind feels the moral obligation to provide the same security measures for persons that assist Red een Kind with our mission as it does for its staff.

In order to ensure compliance to the Red een Kind security measures a person who does not have a contractual agreement with Red een Kind, such as the others as mentioned above, will also have to sign the *Safety and Security Declaration Form*.

The *Safety and Security Declaration Form* states that Red een Kind will do its utmost best to ensure the safety and security of the person as long as he or she complies with the stipulations in this Security Policy and all related documents and/or decisions. The signing of this document does not extend Red een Kind's liability towards this person in case of an incident.

In case of a duty trip, working time will usually be considered to be beyond the actual working hours and it is difficult to distinguish between activities with or without business objectives. This Security Policy therefore applies 24/7 and staff is expected to comply throughout the duty trip (which should take not longer than 4 weeks).

For family members, wanting to accompany a staff member on a field trip, this is only possible after approval from the Operations Director and the before mentioned *Safety and Security Declaration* form will have to be signed.

Towards employees who are, by their own choice, in an area where they were not sent by Red een Kind, irrespective whether or not Red een Kind is active in that area, Red een Kind will not take responsibility. In case an employee wants to combine a holiday with a duty trip, then a clear moment in time needs to be agreed upon that separates the holiday from the duty trip.

Category	Further description of this category	Duty of care of Red een Kind
<b>a. Employees of Red een Kind HQ NL</b>	All travellers having a formal employment contract with ReK.	<ul style="list-style-type: none"> <li>- Sharing written safety and security documentation</li> <li>- If necessary: providing additional oral safety and security instructions</li> <li>- If possible: taking care of a safe and secure working environment/ accommodation abroad</li> <li>- Obligation to arrange for/recommend arranging for travel and accident insurance</li> <li>- Payment of travel and (traffic) accident insurance</li> <li>- Providing for participation in a safety and security course.</li> <li>- ReK has the coordinating role in emergency action</li> </ul>
<b>b. Staff HACA</b>	Local staff having a formal contract with a 100% ReK owned organization.	Same as for <i>category a</i> travelers
<b>c. Self employed consultant (ZZP)</b>	Consultants who assist in ReK's work and offer services that are in line with the work ReK employees are doing. They either travel on their own or under ReK guidance.	Same as for <i>category a</i> travelers
<b>d. Partner Support</b>	Local consultants who assist in ReK's work and offer services that are in line	Same as for <i>category a</i> travelers

<b>Coordinator</b>	with the work ReK employees are doing. They either travel on their own or under ReK guidance.	
<b>e. Members of the Supervisory Board</b>		<ul style="list-style-type: none"> <li>- Sharing written safety and security documentation</li> <li>- If necessary: providing additional oral safety and security instructions</li> <li>- If possible: taking care of a safe and secure working environment/ accommodation abroad</li> <li>- <b>Category e travellers have an obligation to arrange for travel and (traffic) accident insurance themselves, and can ask ReK for assistance in arranging it</b></li> <li>- <b>Payment of travel and (traffic) accident insurance</b></li> <li>- ReK has the coordinating role in emergency action</li> </ul>
<b>f. Volunteers &amp; trainees</b>	No formal contract with ReK and no financial compensation for contribution to ReK activities	Same as for <i>category e</i> Members of the Supervisory Board
<b>g. Groups</b>	Travellers such as donors, junior travelers, schools, entrepreneurs who are always accompanied on their travels by ReK staff .	Same as for <i>category e</i> Members of the Supervisory Board
<b>h. Photographers, journalists</b>	Travellers who offer services to ReK that are not incorporated as such in ReK work and who travel unaccompanied by ReK staff	<ul style="list-style-type: none"> <li>- Sharing written safety and security documentation</li> <li>- If necessary: providing additional oral safety and security instructions</li> <li>- Mention in the S&amp;S Declaration that their profession comes with carrying certain travel safety and security risks under their own responsibility and that ReK assumes them to be aware of those risks;</li> <li>- Recommendation to attend a travel and safety training</li> <li>- ReK has the coordinating role in emergency action</li> </ul>
<b>i. (Employees of) cooperation partners</b>	Travellers from cooperation partners e.g. Woord en Daad, World Servants or Dutch universities travelling with an ReK employee	<ul style="list-style-type: none"> <li>- Sharing written safety and security documentation with the cooperation partner or Dutch university for further use towards travel preparations of category f travellers, including the remark that it is necessary for the category f travellers to arrange and pay for travel and (traffic) accident insurance themselves</li> <li>- If necessary: providing the cooperation partner or Dutch university with additional oral safety and security instructions</li> <li>- Add to contract with the cooperation partner or Dutch university: <ul style="list-style-type: none"> <li>o That they are responsible for sharing written safety and security documentation and additional oral instructions with category f travellers; including a strong recommendation to participate in travel safety and security training</li> <li>o The advice to take care of adequate insurance for their travelling employees/students</li> <li>o To exclude formal liability by ReK and place liability with the cooperation partner or Dutch university</li> <li>o That they are responsible for (involving ReK in) emergency action</li> </ul> </li> </ul>

### 2.3 Compliance

One of the critical success factors for this Security Policy is the acceptance and compliance by all persons involved as mentioned above. Compliance is not optional; it is compulsory and concurrent with the start of any kind of work with Red een Kind. The Security Policy is therefore binding on all persons it addresses. However, in some unforeseen situations staff might be unable to comply with the stipulation when compliance will lead to even greater

direct risks. In those cases consultation with the Operations Director is sought beforehand and a clear explanation is submitted afterwards.

If anyone acts in violation of the Security Policy or any other Security Protocol applicable he or she may be excluded from the activities on behalf of Red een Kind or may face disciplinary actions up to but not limited to termination of the (employment) agreement.

### **3. Principles**

The following principles are the leading principles for security management within Red een Kind:

- Life and bodily integrity of staff has primacy over Red een Kind's assets, reputation and programmes. No material possession is worth risking a life for. Therefore staff should never put themselves or others at risk in order to protect organisational or personal property.
- Safety and Security Management is an integral part of normal operations. It is implemented by line management, which must take security into consideration in all operational decisions.
- While Red een Kind will do every ethical thing possible to secure the release of detained or kidnapped staff, it will not pay ransoms for the release of kidnapped staff.
- Red een Kind will not offer rewards, inducements, or bribes to local officials or others outside the organisation to carry out their normal tasks nor to perform illegal services.
- Red een Kind will not accept the integration of military personnel into its missions, nor the transportation of military personnel (armed or unarmed). Deterrence is a last resort (e.g. in case of an emergency or evacuation). Deterrent measures are only allowed if there is explicit approval by the Board of Directors.

### **4. Responsibilities**

Red een Kind believes that a clear division in responsibilities, communication between staff as well as checks on the application of measures are key factors in managing security in the best possible way. For that, Red een Kind considers the line management structure as the primary system for security management.

The Board of Directors is the overall responsible body for the organisation's security management. The Board of Directors sets the overall policy and makes all final decisions. The responsibility for day-to-day safety and security is with the organisation's line management structure, or representative.

Staff members have the responsibility to ensure their own safety and promote the safety of colleagues. Red een Kind expects from its staff that they understand that all their actions and behaviour can have an impact on the organisation's security position including their own and that of their colleagues.

#### *4.1 General responsibilities of the organisation:*

- To ensure safety and security by implementing a functioning and up-to-date security management structure that can be integrated into the organisation's international business with the aim to mitigate risks. This structure will be laid out in protocols.

- To ensure the security structure meets the requirements of the organisation, that it remains up-to-date and its appropriateness to the organisation's objectives is reviewed on a timely basis.
- To ensure clear lines of responsibilities.
- To ensure the appointment of a Crisis Management Team and a Security Officer.
- To ensure a functioning emergency response system that can be reached on a 24/7 basis.
- To ensure that staff preparing for international travel are incorporated into the security management structure, and receive (but not limited to) a risk assessment, pre departure briefing, pre and post deployment action check lists, medical advice, (medical) insurance, travel contact information and a debriefing upon return.
- To ensure all relevant staff have completed a security training programme.
- To ensure proper (post incident) aftercare when needed.
- To review the Security Policy and protocols on a yearly basis.

#### *4.2 Specific responsibilities of the Board of Directors:*

- To set the overall policy and make any final decisions.
- To decide to establish and to disestablish a Crisis Management Team
- To decide on the use of armed guards and/or armed escorts.
- For the Managing Director to replace the specific responsibilities (as mentioned at 4.3) of the Operations Director during his absence.
- To not travel on an aircraft together.

#### *4.3 Specific responsibilities of the Operations Director*

- To approve specific field trips such as travels to areas that are considered under security level 7 or 8 of the Netherlands Ministry of Foreign Affairs security assessment classification ([minbuza.nl/reisadviezen](http://minbuza.nl/reisadviezen)).
- To withdraw its personnel if risks are deemed too high. Failure of staff to comply with this decision may result in reviewing the staff member's status.
- To ensure that HQ (Zwolle) can be reached on a 24/7 basis (through the emergency number +31 6 2888 5151).
- To facilitate the specific responsibilities (as mentioned at 4.5) of the line management in case of a Field trip for the Managing Director. (in case the Operations Director travels himself, this responsibility is taken over by the Security Officer).
- To facilitate the specific responsibilities (as mentioned at 4.5) of the Management Team in case of a Field trip for Management Team members. In case the Board of Directors travel together this responsibility is delegated to the Security Officer.

#### *4.4 Specific responsibilities of the Secretariat Board of Directors*

- To ensure that staff personal files are up to date and available.
- To ensure that all participants that completed a Safety and Security Training are registered in a database.
- To keep a record (copies) of TRF and RAF (if appropriate) of all staff during travel.
- To keep a record of incident reports.



*4.5 Specific responsibilities of the Management Team (Manager Regio's en Programma's, Manager Kennis en PMEL, Manager FDI and Manager CBF), or representative:*

- To facilitate a relevant and proportional security management structure (including monitoring and evaluation) that can be integrated into the organisation's international business.
- To ensure that the security management structure is followed by adhering to and implementing the organisation's protocols.
- To ensure their staff is adequately briefed, pre and post deployment checklists are respected, travel and traveller's information is up-to-date.
- Sign the Travel Request Form for permission, based on (and discuss with Traveller) recent Risk Assessment.
- To analyse Incident Reports and respond accordingly.
- To inform the Security Officer about the latest developments for the Country Security Plans.

*4.6 Specific responsibilities of staff members (all travellers):*

- To familiarise themselves with and abide by Security Policy and protocols including the organisation's Code of Conduct in order to minimise risks.
- To ensure to receive the latest information about the context the traveller will be working in, as well as any new or on-going security issues and subsequent risk mitigating measures.
- To ensure that staff profile is filled-in, up to date and shared with the Secretariat Board of Directors.
- To ensure that the Travel Request Form is filled in, discussed and signed by management and shared (copies) with the Secretariat Board of Directors.
- To ensure appropriate personal healthcare e.g. medical and dental examination, health advice, vaccination, medicines, prophylaxis and to avoid infection through irresponsible sexual conduct.
- To report incidents to line management within 48 hours in the format as presented in the Travel Procedure, annex 1.
- To withdraw from a mission if the staff member perceives the risks to his/her safety to be too high.
- To demonstrate responsible security behaviour 24/7 during the travel on behalf of Red een Kind.
- To refrain from being the driver of any transportation vehicle during the travel on behalf of Red een Kind in Africa or Asia.
- To make sure that no more than 2 employees of Red een Kind travel in the same aircraft.

*4.7 Specific responsibilities of Partner Support Coordinator and staff from HACA in case of travelling to a foreign country.*

- To familiarise themselves with and abide by Security Policy and protocols including the organisation's Code of Conduct in order to minimise risks.
- To ensure to receive the latest information about the context the traveller will be working in, as well as any new or on-going security issues and subsequent risk mitigating measures.
- To ensure that staff profile is filled-in, up to date and shared with HQ Netherlands.

- To ensure that the Travel Request Form is filled in and shared with HQ Netherlands
- To report incidents to line management within 48 hours in the format as presented in the Travel Procedure, annex 1.
- To withdraw from a mission if the staff member perceives the risks to his/her safety to be too high.
- To demonstrate responsible security behaviour 24/7 during the travel on behalf of Red een Kind.

## 5. Security Management Tools

### 5.1 Security Levels

It is decided to use the Ministry of Foreign Affairs (Buza) Risk Classification System as guidance tool for Red een Kind security related decision-making. It is however realised that as an independent NGO, Red een Kind will make its own decision. Therefore, the Buza risk classification system is used as *guidance*; it is not leading.

(See [www.minbuza.nl/nl/Reizen\\_en\\_Landen/reisadviezen](http://www.minbuza.nl/nl/Reizen_en_Landen/reisadviezen) -Dutch only)

### 5.2 Security Protocols

The following set of documents (Protocols) is developed by Red een Kind in support of the Security Policy. This set of documents will allow its staff to conduct a relevant and proportional security practice based upon the principles defined in the policy.

These protocols are tools for the Management of Red een Kind while implementing the Security Policy and also to support Travelling Staff for practical guidance on Safety and Security before, during and after Travel.

- *Security Protocol 1:* Travel Procedure
- *Security Protocol 2:* Crisis Management
- *Security Protocol 3:* Country Security Plan Manual
- *Security Protocol 4:* Safety and Security Training
- *Security Protocol 5:* Groepsreizen

### 5.3 Security Officer

The Security Officer has no line responsibilities for any security matter. He/she has a supportive role while respecting and stimulating the authority of the Management Team Members. His/her mandate is to:

- Contribute to awareness rising and extension of the Security Policy throughout the organisation.
- Perform an yearly quality and consistency check and report to the Board of Directors accordingly.
- Represent Red een Kind in relevant security networks such as the Dutch Security Network (DSN).
- Developing and reviewing the Country Security Plans.

### 5.4 Crisis Management Team (CMT)

Some security incidents may be of such severity or complexity that they cannot be effectively managed within a normal line-management structure, since this structure might

have become paralyzed by the incident. Such incidents will be managed by a Crisis Management Team (CMT) based at HQ Zwolle.

A CMT is an ad hoc body with the role of managing significant security incidents that:

- are likely to have significant consequences for staff (such as death).
- are likely to have significant consequences for the program in the particular country or beyond (such as program closure).
- are beyond the capacity of the line-management to effectively manage.

A CRMT shall always be activated in the following circumstances:

- Kidnapping/hostage-taking of a staff member
- (Violent) death of a staff member
- Major assault or sexual violence against a staff member
- Increase in security level requiring an evacuation

Other circumstances in which a CMT may be activated include (but are not limited to):

- Relocation/hibernation
- Loss of contact with all/part of country operations
- Imprisonment of an international staff member
- Medical emergency
- Natural/manmade disasters
- Death threats
- Any security incident likely to bring significant media exposure to the organisation

## 6. Annex

### 6.1 Code of Conduct Red een Kind

Staff members of Red een Kind and all other persons not employed by Red een Kind that are working or travelling on behalf of Red en Kind in the exercise of the daily activities of Red een Kind must always:

- 1) Respect and promote fundamental human rights without discrimination of any kind and irrespective of social status, race, ethnicity, color, religion, gender, sexual orientation, age, marital status, national origin, political affiliation or disability.
- 2) Treat all refugees, Internally Displaced Persons, beneficiaries, affected communities, target groups and other persons fairly and with respect, courtesy, dignity and according to the respective National Law, International Law and local customs.
- 3) Create and maintain an environment that prevents sexual exploitation and abuse, abuse of power and corruption, and promotes the implementation of their code of conduct. Managers at all levels have particular responsibilities to support and develop systems that maintain this environment.
- 4) Uphold the highest standards of accountability, efficiency, competence, integrity and transparency in the provision of goods and services in the execution of their job.
- 5) Never commit any act or form of harassment that could result in physical, sexual or psychological harm or suffering to individuals, especially women and children.
- 6) Never exploit the vulnerability of any target group, especially women and children, or allow any person/s to be put into compromising situations. They adjust their own conduct according to the guidelines of the child protection policy.
- 7) Be aware that they represent Red een Kind and act accordingly. They will treat religious and cultural sensitive issues with respect and tact. Employees will be dressed representative, fitting the cultural setting. They will not engage into situations that the partner organization does not consider fitting.
- 8) Ensure that all confidential information, including reports of breaches of these standards by colleagues, obtained from beneficiaries or colleagues is channeled correctly & handled with utmost confidentiality.
- 9) Ensure that reports of breaches of these standards are immediately reported to senior management or the human resources manager (or established agency reporting mechanisms) who are expected to take prompt investigative action.
- 10) Any breach of the Code of Conduct will result in disciplinary action in accordance with the respective terms, conditions and guidelines of the individual agencies.
- 11) Any staff member purposely making false accusations on any action by another staff member, which is in breach of the code of conduct, will be subject to disciplinary action at the discretion of the employer.

6.2 Safety and Security Declaration Red een Kind

The undersigned:

Name:

Residing at (address):

Holder of passport, number:

Declares herewith:

- To travel to (country).....  
from (date departure).....  
up to and including (retour date).....

Regarding activities on behalf of or in cooperation with Stichting Red een Kind (“Help a Child”), George Stephensonstraat 11, 8013 NL Zwolle, hereinafter referred to as “Red een Kind”;

- 1) That he/she has taken knowledge of the Red een Kind Safety and Security Policy, Security Protocols and the Red een Kind Code of Conduct and has raised all necessary questions to Red een Kind for a good understanding and execution of these documents.
- 2) Before and during the period abroad (travelling time included) will fully comply to all arrangements laid down in the documents as mentioned in art. 1.
- 3) All written en verbal arrangements, instructions and orders as mentioned in this agreement will be in force at any time (24/7) unless it has been communicated otherwise explicitly by Red een Kind.

Sign in (place/country):.....

On (date):.....

Name:.....

Signature: