SECURITY

POLICY

2018 Edition

Summary

INTRODUCTION **3**

OUR MISSION 3
Mission *3*
Vision *3*
HUMAN RESOURCES 3
WHY A SECURITY&SAFETY POLICY? 3
DUTY OF CARE 4

COVER, APPLICATION AND TYPE OF THE POLICY **5**

COVER 5
APPLICATION 5
TYPE 5

BASIC PRINCIPLES **6**

DEFINITION OF SECURITY 6
PRIMACY OF LIFE 6
RISK LEVEL AND RIGHT OF WITHDRAWAL 6
EXCEPTIONS 6

APPROPRIATE STRATEGIES AND RISK ANALYSES **7**

STRATEGIES AVAILABLE TO NGOS 7
Consensus *7*
Protection *7*
Deterrence *8*
Recommended Strategy *8*
RISK ANALYSIS PROCESS: BASIC COMPONENTS 8

LEGAL FRAMEWORK **10**

LEGISLATIVE DECREE 81/2008 (UNIFIED TEXT ON HEALTH AND SAFETY AT WORK) 10

RESPONSIBILITY, PARTIES AND TOOLS USED IN SECURITY MANAGEMENT **11**

RESPONSIBILITY AND INTERESTED PARTIES 11
Health & Safety Manager (H&S Manager) *11*
Competent doctor *11*
Security Advisor *11*
Other parties involved *12*
Country Security Manager *12*
Country and Field Security Focal Points *12*
Crisis Management Team *13*
ORGANISATIONAL TOOLS AND SYSTEMS FOR SECURITY MANAGEMENT 14
Risk Evaluation document *14*
ECHO Generic Security Guide 2004 and Cesvi Security Handbook *14*
Risk analysis: Country Traffic Light *14*
Risk analysis: the NGO's Profile in the country *15*
Risk analysis: acceptable risk *15*
Country Security Plan *16*
Annual Report and Annual Budget on Security *16*
Training *16*
Accident and incident analysis *17*
Insurance *17*

ACTORS AND SPECIFIC SITUATIONS **18**

LOCAL STAFF INVOLVEMENT 18
HEALTH 18
General principles *18*
Malaria *18*
Stress and trauma management *18*
Pregnancy *19*
USE OF SYSTEMS AND DETERRENCE INSTRUMENTS 19
Weapons *19*
Armed Guards *19*
Use of private security companies *19*
CRITICAL SITUATIONS MANAGEMENT 20
Attacks, arrest *20*
Abduction and kidnapping *20*
Evacuation *20*
ADMINISTRATIVE ASPECTS AND SENSITIVE DATA 22
Money transfer and management *22*
Document and information protection *22*
COMMUNICATIONS 22
Principles, means and methods *22*
Debriefing and hand over *23*
TRANSPORT 23
Car and motor vehicle use *23*
Flights *24*
SITES AND PREMISES SELECTION 24
PHOTOGRAPHY AND RELATIONS WITH THE MEDIA 24
COORDINATION 25
Joint security management *25*
EISF *25*
INSO *25*
ALLIANCE2015 ..... *25*
Italian Foreign Office Crisis Unit *26*
United Nations Agencies *26*
Civil and military relations *26*
Relations with local authorities *27*
VISITORS, FAMILY MEMBERS, ACCOMPANYING PERSONS 27

FINANCING OF SECURITY MEASURES 28

BENCHMARK 28

POLICY APPROVAL, MONITORING AND REVIEWING METHODS 28

SUGGESTIONS 28

ATTACHMENTS 29

SPECIAL PART OF THE ORGANISATIONAL MODEL RELATING TO HEALTH AND SAFETY IN THE WORKPLACE 29
Incident/accident report form *29*
Incident/accident data form contents: *29*
Early warning *29*
Country security plan contents *30*

APPENDIX 31

SECURITY MANAGEMENT 31
Cesvi's Policy *31*
Different Security Management Models *31*
Job Description *32*

INTRODUCTION

Our mission

Mission

Cesvi operates worldwide to support the most vulnerable populations in promoting human rights, in achieving their aspirations and for sustainable development.

In the name of the ideals of social justice and the respect of human rights, Cesvi works for the wellbeing of the vulnerable populations in conditions of poverty or which have been struck by wars, natural calamities and environmental disasters. This is achieved, at an international level too, through works of humanitarian aid, in the context of both emergency and development, in support of the weakest categories – children, women, elderly and social outcasts –, supporting them in meeting their aims with the objective of promoting self-sufficiency in a sustainable future.

Vision

Cesvi believes that the recognition of human rights contributes to wellbeing for everyone on the planet, a shared home to be safeguarded.

Humanitarian aid and cooperation activities are performed by people for people. Human resources, well-trained and capable of operating in inhospitable and dangerous situations, are what NGOs are really specialised in.

Human Resources

The effectiveness and success of development and humanitarian aid initiatives especially depend on the contribution of the whole staff. The work of an organisation operating in emergencies and development situations places great pressure on its staff. The **Cesvi HR Policy** therefore recognises its responsibility in guaranteeing the physical and psycho-social wellbeing of its staff, before, during and after working with Cesvi[1] .

Why a security&safety policy?

Over the last ten years the context in which Cooperation operates has changed significantly. We have witnessed a progressive and dramatic increase in violence against those who work in the humanitarian sector and against their programmes. Humanitarian organisations and their staff have been direct victims of political and criminal attacks, due to the deterioration of the general social and economic fabric, more noticeably in the developing countries where they operate.

This situation of growing risk led to the need of defining new strategic approaches to the management of safety, to raise the level of professionalism and the coordination tools of the agencies, and therefore to review and update the relevant guidelines, to enable **Cesvi** to act with **humanity, neutrality, independence and impartiality.**[2]

The present Policy is the main enacting tool for the responsibility to guarantee the safety and the protection of its staff through appropriate initiatives (Duty of Care), in the terms of the guiding principles of the **CHS Alliance** (ex *People in Aid Code of Good Practice in management and support of aid personnel)* signed in 2015.

[1] See HR Policy and other Staff Policies and Codes Cesvi, 2008.
[2] The four cardinal principles of humanitarian aid according to the International Red Cross Code of Conduct subscribed by Cesvi in 2002.

Duty of Care

In the last decade the level of fulfilment of the safety standards required of employers for the safety of their workers (Duty of Care) has substantially increased, rendering obsolete and outdated the criteria once considered adequate; this refers to the legal and moral obligation to safeguard employees and those who act on behalf of the organisation from any reasonably predictable risk.

So the **Duty of Care** is the guarantee that in a certain context the employer puts into practice **appropriate measures to prevent and react to any possible incident**, measures that the staff is informed of and is able to carry out adequately.

To this end **Cesvi** undertakes to use methodologies and instruments that can bring to light all foreseeable risks connected to a particular role or activity, establish adequate mitigating and protective measures, develop emergency plans, guarantee staff appropriate information, raise staff awareness and lastly supply suitable support for assisting staff should they fall victims of an incident.

Although Duty of Care is concerned equally with high and low risk contexts, organisations are expected to assume a greater responsibility for staff working in situations or areas considered to be at higher risk.

Since not all risks can be ruled out, the distribution of the **Safety Circular** ensures that the employee is duly informed and consciously accepts the possible risks residual in the work context despite the precautions taken. Nevertheless this document does not represent a release from organisation's responsibility.

COVER, APPLICATION AND TYPE OF THE POLICY

Cover

This security policy regards **all Cesvi staff**: headquarters, expatriate, local, full-time and casual staff, consultants on short or long-term missions, 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 together with the NGO. Cover does not include the following: staff of other NGOs, staff belonging to agencies and governments, company managers and employees, even when involved in Cesvi programmes in some way (these actors are considered external interested parties).[3]

Application

Cover applies to the **persons, property, resources, documents** (including administrative ones) belonging to or available to Cesvi abroad, in all its programmes and under any circumstances. Italian law, TU81/2008, which guarantees the security and safety of staff at the workplace in Italy is taken into account by this Policy solely where applicable to activities abroad.

This Policy does not regard donor relationships, communications, nor does it concern the protection and promotion of the NGO's reputation and public image, which is dealt with in other documents[4].

Type

Adherence to the Security Policy is not optional, but **obligatory** and concomitant with the start of any form of collaboration with Cesvi. The Policy is binding for everyone to whom it is addressed. Any violation of the security guidelines will be considered as a disciplinary violation and dealt with following the terms of the *Staff Code of Conduct* and the *Ethical Code* in the procedure for the *Transparent management of complaints*[5].

[3] However, any conduct or decision of external interested parties which places Cesvi staff, property or resources at risk, shall be duly dealt with by the Cesvi staff; so that risk is minimised as far as possible both for themselves and Cesvi.

[4] Management of relationships with individual donors, Manual for Visibility and Communication, IV Edition; Policy for use of images of children and young people; Privacy Policy etc. All the documents are available both in English and Italian.

[5] See: Human resource Guidelines and other Guidelines and regulations for staff, Cesvi.

BASIC PRINCIPLES

Definition of security

Security management must always be fully integrated within projects, thus contributing to ensuring that **the objectives of the initiatives in the field are met**, whether they be for emergencies or development. This means that the maximum level of safety and protection of staff must always be matched with the meeting of obligations taken on towards beneficiaries and other interested parties (donors, service providers, etc.).

Security management must be developed so as to provide flexible options suitable for conditions and risks of the various situations.

Protection and security are achieved, subsequent to an evaluation of risks existing in any given context, when the following conditions are met:

- - staff are protected and able to operate in safety;
- - property and resources (equipment, financial, local, documentary resources) are all protected at the highest possible level.

The implementation of the security measures contained in this Policy and related documents does not weaken the achievement of the aims of the development cooperation and humanitarian aid, nor does it jeopardises the effectiveness and the efficiency of the programmes and projects, but actually makes their achievement more feasible and increases their quality.

Primacy of life

Decisions and actions regarding staff security, protection and health take precedence over any activities aimed at preserving property, equipment, financial resources, documents or infrastructure.

Risk level and right of withdrawal

Staff are always informed beforehand of the level of risk of any given mission and have the right to withdraw at any moment. In the interests of security and after discussion with their Operational Contact Person, any member of staff, regardless of their functions or the opinion of the **Cesvi Security Advisor** or their Contact[6], may decide to withdraw from an area or interrupt an activity. **Cesvi** will do anything possible to facilitate the withdrawal and will not charge the member of staff in question any cost incurred in the withdrawal stage.

Staff who do not feel able to cope with the level of risk of a certain activity or position may ask their Contact to be assigned to other activities or positions. Within the terms of the contract, Cesvi will do anything in its power to comply with such request.

Exceptions

Every exception or waiver to what is specified in the Security Policy may only be authorised by the CEO & General Manager in writing to the Security Advisor, to the Supervisory Body over expatriate staff and to the interested parties. Should the CEO-GM not be reachable this responsibility will be taken on by the President, who may consult the Board, whose decision will be made with a majority vote.

[6] The Operational Contact Person (the Contact) is the person, indicated in the document formalising the worker's relationship with Cesvi (employment contract, voluntary worker, etc.) or in the Job description, to whom the worker must report during operations.

APPROPRIATE STRATEGIES AND RISK ANALYSES

Strategies available to NGOs

Theoretical analysis and experience over recent years coordinating security have led to the identification of three main management approaches: **consensus (or** acceptance**), protection** and **deterrence**.

Consensus

Consensus (or acceptance) aims to **reduce or remove the danger** of operating in a particular context, **enhancing the** appreciation **of the agency** and the work it carries out.

Consensus is unanimously considered by all NGOs to be the approach that suits the aims of humanitarian and co-operation organisations best. Just as a good development or emergency operation cannot be completed without the creation of a consensus with the interested parties involved (starting with project recipients, social groups interested in any way and local authorities), it is unthinkable that high levels of protection and security can be maintained without counting on the positive image that NGOs manage to earn for themselves in the places where they operate.

Consensus is not just something that happens on its own but is part of a **complex strategy**, the success of which depends on:

- - the use of a model that adds value to shared processes, increasing participation, transparency, sustainability and the management of suggestions and complaints;
- - the reputation of the NGO and its credibility as a development and humanitarian aid actor;
- - the quality of the staff selected;
- - the reputation and reliability of the partners and local actors working together with the NGO;
- - the quality and importance of the programmes carried out;
- - the ability of the NGO to communicate what it is doing in every way: reports, visibility, media use, administration, HR management etc.

The attitude of the local population towards international organisations with which NGOs are often compared must also be taken into account.

An organisation which has attained the highest degree of acceptance possible in the area where it operates is generally a safeguarded organisation, safe from the majority of risks, counting as it can on numerous protective factors offered by the community where the NGO operates.

This is often not enough to guarantee maximum security, however, where risks requiring different solutions exist: an area with a high frequency of natural calamities, for example, or the presence of criminal groups indifferent to the NGO's role.

Protection

Protection is the second most widespread approach adopted by the majority of NGOs.

A protective approach uses defence devices and procedures to **reduce vulnerability** to the threat of staff, goods, equipment, documents and infrastructures, but is not able to reduce the threat itself.

This approach may be followed in two ways: reinforcing the objective or changing the visibility level (a greater or lesser visibility may be strategically more or less adequate according to the context).

An example of this type of approach are the measures taken to protect premises by NGOs, such as window bars, night-time lighting etc., or those regarding transport and communications, such as modern,

secure vehicles or reliable communications systems. The training and rules of behaviour of local and expatriate staff must also be taken as protective measures.

Deterrence

However in various countries NGO's neutrality goes unrecognised. Ever more frequently they are victims of aggression, kidnapping or attacks by various types of criminal or terrorist groups, to such an extent that this sort of violence represents the main risk factors for humanitarian staff.

In this context it is therefore necessary to add **deterrence** to the measures for managing risk by way of threat **containment**, or **contrasting it with a counter-threat**. Strategies of deterrence include resorting to armed guards and bodyguards, the threat of abandoning the area breaking off programmes and help, the use of private security-management companies etc.

A deterrence is therefore a counter-threat expressed in legal, economic, political or military terms. Its purpose is not so much to act on risks generally and implicitly or explicitly on vulnerability, as to use a counter-threat openly to halt or slow down the original threat.

Recommended Strategy

In the light of their mission and the principles and values that they hold, NGOs tend to prefer **consensus as the most appropriate strategic approach**. Actually, even though it is the basis of the security strategy, it cannot be effective against all threats. In places where crime, banditry and terrorism are rife, where warring factions pursue national or global objectives and where the objectives of the aid agencies are not recognised, the consensus approach alone cannot be sufficient.

But on the other hand nor are protection and deterrence free from problems. In adopting the protection approach the agency identifies itself as a potential target, running the risk of generating a paranoid "Bunker" mentality, which can prejudice relationships with others including those of the communities being aided; resorting to the deterrence approach, which implies the use of armed escorts or guards may be in contrast with the claim of the organisation's principles of non-violence and independence, to the point of the risk of appearing aggressive.

It follows that a security strategy requires a **flexible and balanced combination of various approaches to the problems**, that can be effective only if developed around the characteristics of the environment in which it will be used, and only if the organisation has the ability and the skills to manage it adequately, keeping it up to date and adapting it in the light of the evolution of the context and the relative risks. In no case is it possible, whether using a single strategy or a combination, to reduce the risk to zero.

Lastly it must be borne in mind that, independently of the approach or mix of approaches one decides to adopt, there will be a cost and a constant obligation will be required on the part of the organisation in the allocation of resources, even those not necessarily related to the security sector (programmes, operations, human resources, etc).

Risk analysis process: basic components

Risk analysis involves **establishing the level of vulnerability** of a person, an organisation, of its goods and property and its programmes, to a specific innate danger in the context of putting the activity or project into practice.

This exercise makes it possible not only to develop a series of measures capable of mitigating the risks, but also to evaluate them in comparison to the help that the project will bring to the beneficiaries. Responsible management – of oneself as well as of others – implies the commitment to avoid endangering uselessly persons or goods, namely not to expose them to risk out of all proportion with the impact of the help they claim to bring to the beneficiaries.

The risk analysis must be treated as a living document, and as such must undergo **periodic revisions and updates**, based on significant changes in the operational context, and in any case when the activity in question is to start, to end, or to be expanded, or at times of special events (such as electoral campaigns, threat of social or economic instability, forecast of particular climatic conditions, etc.).

From another point of view the risk can be defined and measured by objectively calculating the probability that a given threat might occur and the potential impact on the persons directly involved (physical, moral or psychological damage) or on the organisation as a whole (scheduled activities, economic damage or damage to the image or reputation, etc.).

The risk analysis must lead to the implementation of a **series of mitigating measures**, as per the approach chosen by the NGO. These measures may have the purpose of reducing the NGO's weaknesses, increasing its strengths, changing its activities and/or changing its area of operations, etc.

No security measure can generally cover all risks. The best solution is a combination of several actions, generally including the following:

- **withdrawal:** no further action
- **control:** use of preventive measures *against* or mitigation *of* risk
- **distancing:** temporary distancing of the threatened target
- **transfer:** the risk is shifted to other actors (insurance companies, sub-contractors, partners).

This last option should be extremely carefully considered, as the moral responsibility for assessing the consequences of the transferred risk would be Cesvi's. The decision to run a mission by remote control or distance management is always taken at the highest level, therefore (CEO and COO), implicating as it does the transfer of the risk to local partners or operators.

LEGAL FRAMEWORK

Legislative decree 81/2008 (Unified text on health and safety at work)

Cesvi has already conformed to the rules contained in the ex law 626/94, which is now absorbed and expanded by the Legislative decree TU 81/2008 updated in May 2017, which establishes for all the bodies under Italian law specific measures for the safety and protection of personnel.

Cesvi headquarters have consequently drawn up a Risk Evaluation Document.

The Employer has appointed[7] the Health & Safety Manager (H&S Manager). Also a Workers' Security Representative and first aid and fire prevention staff have been appointed as per TU81/2008 specifications. A competent doctor has also been appointed. The qualifying courses needed to be able to perform these functions have been organised as required by law. These courses are repeated at regular intervals, again required by law.

In the headquarter the CEO-GM is directly responsible for the application of the safety measures with the help of his delegate, in the particular case the Head of Finance, who has received the mandate on August 1st 2016.

The Board of Directors has decided that the H&S Manager must make use, for anything concerning institutional activity abroad, of a **Security Advisor**, nominated with a specific mandate, for counsel and monitoring work. Such activities, besides being prevalent, are also the most exposed to various types of risk.

[7] Update of nominations 2017.

RESPONSIBILITY, PARTIES AND TOOLS USED IN SECURITY MANAGEMENT

Responsibility and interested parties

Cesvi believes that the **distinction between responsibilities**, **communication between staff** and **checks on the application of measures** are key factors in managing security and protection in the best possible way. All staff members are therefore called on to recognise their own personal responsibilities regarding security and to make contributions of their own within these three contexts.

All staff must constantly be alert to questions relating to security and protection. The existence of specific services and responsible parties does not exempt any member of staff from:

- understanding and implementing security measures;
- being alert to risks and security concerning their team;
- being responsible for their own security and that of those under their management;
- behaving positively as a member of Cesvi, by promoting the Cesvi Staff Code of Conduct;
- share in the creation of a "Safety culture";
- reporting any action or breach of the Security Policy and related documents to their Contact Person. (Also see under paragraph, Organisational tools for security management);
- using their judgement[8], wherever security measures are weak or inapplicable.

Health & Safety Manager (H&S Manager)

The **Health & Safety Officer** is the figure provided for by Italian law to be in charge of company security problems (non profit companies included).This figure has four tasks: identifying dangers and eliminating any consequent risks, supervising the drafting of the Risk Evaluation Document, training staff and promoting workers' health.

In Cesvi the figure of Employer is taken on by the CEO-GM, who, on August 1st 2016 delegated the role of H&S Manager to the Head of Finance who, for activities abroad, uses the Security Advisor.

Competent doctor

The **competent doctor** is the figure provided for by Italian law to supervise staff health problems.

Security Advisor

All security measures are to be applied abroad by all Cesvi staff operating in close co-operation with the **Security Advisor**, who was delegated by the Employer on June 19th 2017, in terms of the article 16 of the legislative decree 81.

The Security Advisor reports to the CEO-GM and his job is **to advise and support expatriate staff**; this figure monitors the effectiveness of the security measures adopted by the NGO in the various countries where it operates, and gives the CEO-GM his/her assessment.

The Security Advisor also draws up **general or specific recommendations**. These recommendations, authorised by CEO-GM, are communicated to the relevant staff. The recommendations are drawn from analyses of situations, incidents which have occurred or from information shared with the security networks, with which the Security Advisor is constantly in contact. As they are issued, the recommendations become

[8] It may be useful to remember the summary proposed by Medici con l'Africa CUAMM, in order to understand what is meant by judgement: 1. observe and be careful and cautious; 2. Pay attention to your own impressions; 3. change habits frequently (routes and times); 4. be respectful but not submissive; 5. keep calm; 6. never put your own life at risk to defend material resources.

an integral part of this Security Policy. Where necessary the Security Advisor may be deployed abroad and assume on a temporary or permanent basis the role of Security Manager.

The job description of the Security Advisor is specified in the Appendix.

Other parties involved

The security measures in Italy and in the field are applied as per Cesvi's operating structure. While the General Manager at headquarters is therefore directly responsible for the application of security measures in Italy – with the support of his delegate, in the particular case the Head of Finance, who received the mandate on August st 2016 – security measures abroad are applied following the operational structure hierarchy, from the General Manager to the COO Chief of Operations, to the Area Desk together with the country's Head of Mission, down to the Focal Points for safety present in every country (or area within the country).

In higher-risk countries, a specific figure, the **Country Security Manager** (CSM), is also provided for.

Where it is not possible or necessary to hire a dedicated CSM the role will be assigned to a team of staff who, coordinated by a team leader, will act as focal points of the security structure. The composition and specific working procedures of the team will be defined at the level of the single country, following the generic guidelines, and with the support of the Security Advisor.

To be able to carry out this role the staff must be have the will and attitude, and must also receive sufficient support, training and recognition from the organisation in order to simplify the addition of this task to their normal activities. Personnel who are responsible for security must have their functions clearly formulated in individual terms of reference and in the evaluation and performance parameters.

The Security Advisor plays a stimulating, addressing and checking role with respect to the operating structure.

Country Security Manager

This is the person in charge of the management and supervision of security measures in **higher risk countries**: she/he makes risk analyses, circulates information and trains staff in loco.

This role cannot generally be compatible with that of the Head of Mission (except in particular circumstances and with prior approval of the CEO-GM) since, among other factors, the responsibility for control, support, advice, training and representation on security matters are to be held separate from other management or representational roles. It may be entrusted to expatriate or local staff with tasks of a preferably logistic nature. The Country Security Manager answers to the Head of Mission, and consults and seeks advice from the Security Advisor (for the JD see the Appendix).

Country and Field Security Focal Points

In every country a **Country Security Team (CST**) is set up, composed of the Country Security Focal Points and coordinated by a Team Leader.

The CST collaborates in the development and revision of the security policy, in the determination of the minimum safety requirements and the revision of the organisation's security procedures; the team also supports those responsible for putting into practice and in management control of the safety risk as to the parameters and equipments at their disposal in the country; lastly, it ensures that the plans for crisis management are drawn up, put into practice and periodically tested.

The Security Focal Points (SFP) which compose the CST must be selected in order to form a heterogeneous group, which includes national and international staff, and a balanced number of men and women, so as to be representative of all mission's workers.

Every SFP, within the specific context of the country security structure, collaborates with the mission to **promote staff safety** and guarantee that the security policies and procedures in force are known and respected.

The SFP is responsible for the **collection and diffusion of reliable security information** which can contribute to the updating of the context analysis: the SFP also keeps colleagues informed, thus contributing to the creation of a security culture.

Crisis Management Team

In the case of serious crisis situations, incidents or the threat of serious menaces, Cesvi activates its own **Crisis Management Team (CMT**), whose operational guidelines are laid out in the *Cesvi Crisis Management Plan* and *Crisis Management and Communications*.

The team, presided over by the CEO-GM, remains active for the whole duration of the crisis and meets up informally and by any means (including electronic). It is made up of the following:

CORE TEAM

- CEO-GM
- COO
- Security Advisor

CMT

- Head of Project Dept.
- Head of Finance Dept.
- Head of Human resources
- Head of Legal and Internal Audit Dept.
- Emergency Coordinator
- Desk Officer of the country being involved in the crisis
- any other person who the Core Team decides may contribute to the management and solution of the crisis (e.g. the President, Head of Mission, Country Security Manager or any other Cesvi staff member in the Country affected by the crisis).

The following are examples of the problems the Team responds to:

- death, serious incident or illness of a staff member;
- relations with the next of kin of staff who have been victims of a serious incident;
- disaster or other event that prevents the central or local headquarters from functioning regularly;
- interruption of communications with one of the foreign bases or serious IT malfunctioning at headquarters;
- serious fraud or theft (refer to the Anti-corruption Policy);
- kidnapping;
- claims for damages arising from accidents.

The Team also deals with any other event which the CEO decides may need to be dealt with, including those proposed by other members of the Team.

The CEO reports to the Board of Directors on the Team's activities and submits all matters regarding the latter for approval to the Board of Directors.

The CEO may authorise the creation of a Crisis Team in loco to manage any contingent situations, by calling on the most appropriate staff to deal with the crisis in the Country in question.

Organisational tools and systems for security management

For security and protection management the following **organisational tools and systems or pre- requisites** are available to staff:

- - this Policy, illustrating the basic guide lines and division of responsibilities;
- - a Risk Evaluation Document (solely for headquarters) as per TU 81/2008;
- - a General Handbook regarding staff security abroad: ECHO, Generic Security Guide, 2004;
- - the *Operational Security Management in Violent Environments* manual by the Humanitarian Practice Network (HPN);
- - a Short Handbook: Cesvi, Security Handbook;
- - a manual and a Power Point presentation for training on the "Circle of Security" methodology (based on the training manual by IPSO, Somalia)
- - a document for brief definitions of a country's specific risks (its "traffic light") and definitions of the profile to be used in each country;
- - Country Security Plans for all countries
- - Annual security report;
- - general budget for security measures and training;
- - training plan;
- - collection and analysis of accident and incident data concerning staff;
- - suitable forms of staff insurance and health cover for each country;
- - compliance with the provisions of the Organisational Models defined in the Legislative Decree 231/0;
- - reporting duties to the Supervisory Body as defined in the Legislative Decree 231/01.

Risk Evaluation document

Provided for by TU 81/2008. Concerns analysis of risks regarding headquarters. This document is compulsory by Italian law. It is updated by the H&S Manager.

ECHO Generic Security Guide 2004 and Cesvi Security Handbook

These two documents, being the former more general and complete while the latter simpler and more immediate, are the **main operational references** regarding the management of generic security measures for all staff. In particular, in the two documents staff feeling unprepared in unexpected situations can find useful check lists advising on the best actions to take.

The Cesvi Security Handbook is a simple tool for the management of non-specific security related situations. It is used by Cesvi as a reference handbook when more appropriate tools are not compulsory (such as the Country security plan). It has the major advantage of being available in English and French and being easy to consult.

Risk analysis: Country Traffic Light

Risk analysis is the process that lies at the heart of the Cesvi Security Policy. Its aim is to reduce vulnerability before any concrete threats can actually occur, by dealing with the risks most likely to occur first, while never neglecting less probable ones, especially if they may have a great impact.

As stated above, it is part of the Security Advisor's brief to maintain and direct this process and glean suggestions and conclusions from it.

One of the risk analysis tools in Cesvi is the **Country Traffic Light**.[9] This is a simple table where different colours (Green, Yellow, Red)[10] indicate the different risk levels for the countries where Cesvi operates. The attribution is made by the country securiy team on the basis of two sets of parameters, relative to safety and inconvenience; whenever requested, the Security Advisor must give adequate support during the analysis process and ratify the final attribution. The tool is updated whenever felt necessary, at least a couple of times a year.[11]

Risk analysis: the NGO's Profile in the country

It is not possible to draft a Country Security Plan without establishing in advance, at the start of the mission or as soon as possible, both the **project aims and limits** within which the resources and the activities that the NGO intends to develop are located, and the **type of visibility** of the NGO in the given country.[12]

The choice of Country Profile type (high or low project input; high or low visibility) is decided by the COO *Chief of Operations*, the Head of Projects Department and the Area Desk, since it influences the whole structure of the security measures adopted in the country from the foundations up. The decision is made together with the Security Advisor and the CEO-GM and may be reviewed if necessary. Every review entails the updating of the Security plan to include the new profile. The choice of Country Profile implies the definition of acceptable risk level in that country.

Risk analysis: acceptable risk

In the most critical situations, the process described briefly above also aims at the definition of an **acceptable risk**, that is, a **threshold** beyond which it would be better introduce risk mitigation's actions or to withdraw:

- would the consequences of implementing the programme be so serious as to justify the acceptance of such a risk?
- have all possible alternatives been explored to attain the aims of the programmes?
- has every effort in terms of human and financial resources been made to lower the risk to a medium level?
- what strategy has been used in order to prevent non-eliminable risks from growing further?
- what would be the consequences of failing to implement the programme or its interruption ?

The check of the acceptable risk level is a responsibility of the Security Advisor. When in a Country, considering the programmes implemented, the assessed risks are higher than the acceptable threshold, the Area Desk, the Head of Projects Department and the COO *Chief of Operations* are notified by the Security

[9] The tool is similar to others in use at other NGOs.

[10] Red indicates the presence of several high-level risks in the country. A specific Country Security Plan, with detailed recommendations regarding security and emergency management in that country, must be in force in order to deal with them, therefore. It also indicates that a member of staff has been chosen to cover the role of Country Security Manager. Staff should not be accompanied by family members during missions in these high-risk countries (no family duty station). Yellow indicates that the country is under special observation for the assessment of new risks. A specific security Plan must be introduced or the indicator must be restored to the lowest level as soon as possible. Green indicates that the country is considered a low risk destination.

[11] The General Manager and the HR team take the various risk levels into account (colours) when calculating the benefits (economic or otherwise) due to staff abroad or on short missions.

[12] Operating in a Country where NGO activities enjoy a wide consensus and programmes are carried out with a wealth of resources, which imply a high profile in terms of visibility and project input (numerous staff, significant economic resources, explicit and wide-spread relations with interested communities and authorities, etc.) is one thing. Quite another thing is when a low profile has to be kept, with little or no visibility, and project input is limited (relations solely with interested and closest groups, limited economic resources, staff reduced to the strictly indispensable, etc.).

Advisor. The heightening of the threshold of acceptable risk involves Cesvi's highest ranking officers, those of the greatest responsibility: Board of Directors, President, CEO-GM, requested by the Head of Projects Department, and the COO *Chief of Operations* or by the Security Advisor.

Country Security Plan

The **Country Security Plan** is an essential document for the day-to-day management of security in high-risk countries. No Country Plan is the same as any other, because each one must correspond to the specific conditions under which Cesvi operates in the country in question. **Risks most likely to occur**, or possibly those with greater impact are identified for the Plan by analysing the context of where NGOs work in the country, or that of a specific area. It also describes preventive measures for managing the risks or the reactions to threats that could occur.

Drafting and updating the Country security plan is the responsibility of the Head of Security in the country in question, with the support of the Security Advisor. The Security Plan is to be updated at least once a year, and in any case whenever changes occur that make the edition in being ineffective.

The process of drawing up the Country Security Plan must be shared, including programming and operative staff at all levels (managerial and in the field), national and international staff with an adequate gender balance in order to respect – in the analysis of risks and proposal of solutions – the points of view of all interested workers.

Cesvi provides Guidelines for the writing of the Plan (WORKSHOP manual for writing the Plan).

Annual Report and Annual Budget on Security

The **Annual Security Report** is drawn up yearly by the Security Advisor and summarises, for the employer, the Board and the Supervisory Body all that has happened during the year concerning the security of the ONG. It is accompanied by a final balance sheet.

The Security Advisor prepares a summarised planning annually accompanied by an estimated Budget aimed at covering the general security costs sustained by the NGO headquarters.

An example of the contents of the annual security report can be found in the attachments.

Training

The application of security measures must be sustained by a **process based on participation and care**, bolstered by training sessions. Cesvi is committed to drawing up a Security Training Plan. The Security Advisor is in charge of drafting and reviewing this plan, which specifies timing, contents and training recipients, delivery methods and trainer features in detail.

It must also concern:

- basic pre-departure training for all expatriate staff (regardless of the type of employment and responsibility);
- specific training for staff assuming the role of Country Security Manager in loco;
- the possibility and the criteria allowing staff to take part in general or specific training organised by official parties, with or without Cesvi's contribution to costs;
- specific training for all staff, including local staff, in the countries where a Country Security Plan (high-risk countries) is in force.

The Plan, reviewed whenever necessary, is an internal document and also contains at least:

- information on the contents of the basic pre-departure course, of the Country Security Manager course, of the course for staff allocated to high-risk countries: timing, contents, trainers;

- a list of the parties offering specific training and information regarding the possibility or otherwise of using it;
- information about courses carried out in loco: contents, methods, trainers.

The participation of family members, journalists, staff of other NGOs or others interested in the training courses held by Cesvi is subject to the approval of the Security Advisor. Cesvi sustains the costs for the training it provides.[13]

All persons trained are obliged to contribute to the application of Cesvi security measures, within the limits of their abilities and responsibility.

Accident and incident analysis

An analysis of the accidents and incidents that occur most frequently to the NGO's staff is useful for improving the training and the promotion of increasingly suitable protection and security measures for dealing with the risks to which the NGO is subject. The Security Advisor's job is to keep the NGO accident and **incident data base** up-to-date, and also includes the drafting of a specific chapter in the annual report. Operators must, within 48 hours, communicate, directly or through their contact person, events (regardless of the cause: health, accident or violence) which have affected the organisation in some way. If considered important, this information should be extended to facts regarding other NGOs with which Cesvi has relations in the same operational area. A simple form is available for such information.

Reporting and incident analysis is included in the training.

The report is to be made to the Supervisory Body annually, except in cases of serious work accidents with prognosis more than 40 days, in which case communication is immediate.

Insurance

All expatriate staff operating for Cesvi (regardless of the type of employment or responsibilities) have **insurance cover** against illness, accidents, third-party liability, death, urgent medical evacuation, and repatriation for health reasons, which also covers cases of war.[14]

In the event of staff having their own insurance policies, Cesvi will assess in any case whether to extend its own standard insurance cover. If not, operators will be required to explicitly waiver their right to the insurance policy offered by Cesvi. Insurance premiums stipulated by Cesvi are payable by Cesvi.

Staff must always provide the names of persons to be contacted in case of emergency (next of kin).

Insurance cover for all staff hired in loco is defined locally, as per local laws and customs. Cesvi HR Policy also establishes that all Cesvi staff must have accident and pension insurance where it is not provided for by local labour laws. Appropriate budgets must be included in all projects.

Local staff operating in areas other than their original engagement (see "Evacuations") are included in the staff category paid for by Cesvi in the event of medical evacuation, through special insurance cover or ad hoc agreements with companies specialised in urgent medical evacuations.

Staff should ask the HR Team or their contact person for clarification regarding their insurance cover.

[13] Journey, accommodation, teaching and teaching materials.

[14] The insurance covers chosen by Cesvi are some of the best available. Nevertheless they also have some exceptions: individual staff members are responsible for checking the contents and the limits of the insurance policies concerning themselves.

ACTORS AND SPECIFIC SITUATIONS

Local staff involvement

Defining, applying and checking security measures is never a simple or limited process: it interests all the staff and all the aspects of any Cesvi mission. Cesvi believes in training sessions to make local staff aware of their responsibilities (see HR Policy): the greater the collaboration the higher the security. Local staff involvement will always be required, whether during the identification of security tools or training and application stages, right up to the checking stages.

Health

General principles

Operational conditions expose staff to **health risks**. Cesvi has therefore drawn up a detailed system for the proper management of health protection. It comprises the following:

- - blood tests (specified by the competent doctor);
- - a list of vaccinations recommended for each operational area;
- - medical examination made by the competent doctor's to establish suitability for the country of destination;
- - doctor's check of vaccination validity;
- - insurance;
- - stress and trauma management methods (psychological support);
- - rest period programming (specified in employment contracts) and R&R[15] in particularly stressful missions;
- - social and health insurance for the local staff according to the local labour regulations.

The single security tools or organisational systems (Protection plan, Security plan, etc.) for single countries must dedicate adequate attention to preventive health, diagnostic and treatment measures that can be activated for staff in local contexts (like for example the stipulation of insurance policies or agreements with local clinics).

Malaria

Since this is one of the most dangerous tropical diseases, Cesvi is especially careful to inform staff designated to work in countries considered to be at the highest risk.

Stress and trauma management

Staff are offered two ordinary methods to deal with **stressful situations** linked to their development cooperation activities and humanitarian aid.

The operator's contact is the first person in charge of managing signs of stress or trauma. Expatriate staff can also always access an expert psychologist via the HR team, who will deal with the operator's questions with discretion.

Serious episodes of a traumatic nature must always be communicated to the COO Chief of Operations and the Security Advisor, who will decide whether to consult the Cesvi Crisis team. The Security Advisor checks and investigates operational conditions in order to identify the causes of stress and to prevent them.

[15] R&R: Rest and Recuperation. Specific application methods are decided on a case-by-case basis (also see Human Resources Policy).

A specific section of the Risk Evaluation Document id dedicated to work-related stress

Pregnancy

Working in humanitarian and development cooperation projects while **pregnant** does not have any effect on the results achieved, but is often inadvisable because of the environmental risks and the appropriate related measures proposed to combat them, like in the case of vaccinations, which can sometimes be incompatible with pregnancy.

Being pregnant implies a wider and deeper assumption of responsibility by the staff member, in order for the security measures and protection concerning them to be managed in the best possible way:

- preventive treatment for the international traveller: journey, stress, vaccinations, medicines;
- assessment of the risks specific to the area of destination;
- assessment of tasks.

In compliance with HR Policy, Cesvi informs its pregnant staff of the general risks that they are running while simultaneously offering the maximum support possible.

Use of systems and deterrence instruments

Weapons

Carrying weapons (fire-arms, knives, explosives) puts at risk the **position of neutrality and impartiality** that Cesvi tries to maintain in all contexts.

The presence of weapons constitutes a risk for the security of the staff and those operating with them (programme recipients).

Therefore Cesvi staff are not permitted to carry weapons.

No armed person may have access to vehicles or premises (even leased) which fall under Cesvi's responsibility. Cesvi will do everything in its power to have any type of weapon banned from any environment where the NGO operates.

Armed Guards

Due to the fact that Cesvi follows a non-deterrence-based security approach, it avoids using **armed guards** or **escorts** to perform its activities.

Nevertheless in some circumstances the use of armed guards may be required by governments of the countries where Cesvi operates as a precondition to authorising the NGO's operations, or they may be necessary in order to deliver urgent humanitarian aid in openly threatening situations.

In these situations, and in all cases where the need may arise, only the COO, working with the Security Advisor and with adequate information from the interested Area Desk, may consent to an **exception**, based on a specific risk analysis, to permit the use of armed guards or escorts: this is to be ratified by the CEO.

Authorisation is always linked to a specific situation and cannot be generalised to include other similar situations. In no case may such guards or escorts ever be employed directly by Cesvi. They must be part of military bodies, police, or security bodies recognised by the country hosting the NGO.

Use of private security companies

Making use of **private security agencies** for surveillance is permitted as long as it meets the requirements and the security measures set out in the preceding paragraph, conforms to the law of the host country and does not violate the behaviour codes to which the organisation adheres.

Critical situations management

Attacks, arrest

The **prevention of attacks** (such as robberies, intimidation, sexual aggression, etc.) is an essential component of the training and protection and emergency health Plans of all the countries where Cesvi operates.

To this end each Plan must include an analysis of the risks and the methods of preventing them: avoid certain areas in certain hours of the day, avoid certain places, avoid routine routes etc. In the event of attacks against a staff member, the persons informed of the facts, that is the person with the highest degree of responsibility in the country, must send a **detailed report** to the Security Advisor, highlighting the measures to be taken to prevent the recurrence of similar events.

In the event of the arrest of any expatriate staff members, Cesvi will inform the consular authorities and decide on the action that will **achieve their release in the shortest time possible**. It will also contact a lawyer to assist in the case, if necessary. It will also see if conditions exist to inform the International Red Cross. Similar actions are put in place for local staff.

Abduction and kidnapping

Abduction and kidnapping are two of the **most serious threats** that NGO staff must face.

Cesvi's basic training for staff leaving for countries where this risk is widespread includes a specific section on how to deal with or prevent this occurrence. The Country Security Manager is responsible for implementing a training session in loco for all local staff.

Should a Cesvi staff member be kidnapped, Cesvi headquarters must be informed as quickly as possible.

The Core Team will activate the Cesvi Crisis Team to organise the following:

- contacts with family members;
- contacts with the relevant authorities (if necessary, also the Italian Foreign Office Crisis Unit);
- if necessary, the choice of a mediator;
- contacts with the media;
- choice of the best strategy of interacting or otherwise (if necessary) with the kidnappers, even when no specific ransom request has been made.

Evacuation

Every Security Plan should include specific information on the **proper management of an evacuation** and its preliminary stages, by taking into consideration the specific conditions of the Country in question.

The Plan must also include the following lists:

- a list of expatriate staff;
- a list of local staff living and operating in the area where they have been hired;
- a list of local staff operating in any different area from where they have been hired or from where they come.

The evacuation plan must include specific implementation methods for each staff category. Cesvi is responsible for the evacuation of **expatriate staff**, which will follow the indications contained in the Security Plan of the area in question or other methods defined by Cesvi.

Cesvi is responsible for the evacuation to safer areas of its national (local) staff operating far from the area where they come from.

Cesvi is not responsible for the evacuation of Cesvi staff who come from the area where they are operating. However, if specific risks for the safety of this staff have been identified in advance, Cesvi will do everything possible to facilitate their evacuation to protected areas, by using the resources of the Country in question.

All the above-mentioned staff categories will be informed of the procedures to be followed in the event of evacuation according to the category to which they belong during the security training sessions in loco.

The ECHO Generic Security Guide and Cesvi Security Handbook documents include useful recommendations for the management of the different and most common situations. Staff must refer to the Security Advisor for any other information.

In all cases **evacuation procedures** must identify at least the following:

- property, equipment, documents and staff to be evacuated in the event of pre-evacuation[16] (non-indispensable staff and property and resources difficult to evacuate in cases where the situation is deteriorating rapidly);
- which staff, with what resources and responsibility are left in loco;
- the amount of the salary to be paid in advance to the local staff (number of months);
- programme suspension methods.

As mentioned at the start of this Policy, no operator, whether local or expatriate, may be pressurised into continuing to work for Cesvi.

Good selection and monitoring of staff skills and results should easily identify those that can be counted on in critical situations.

The temporary **hibernation** of activities in an area (either leaving staff in place, due to the dangers in removing them or proceeding with a **complete or partial staff evacuation**), is decided by the CEO-GM and the COO Chief of Operations, at the request of the Security Advisor or of the Area Desk.

Decisions regarding **withdrawal** from a country or the **resumption of activities** in a country that had been partially or completely evacuated are similarly taken.

In this last case, a review of security measures in the area prior to a complete resumption of activities must be effected as soon as possible.

Cesvi acts solely **in the interests of its staff and programmes** when taking the above-mentioned decisions, but also assesses information and indications from numerous parties (such as the United Nations, European Embassies, Local Authorities and partners, Italian Foreign Office Crisis Unit, other NGOs and other international organisations, etc.). Again, in the event of evacuation "orders" issued by local authorities, Cesvi acts in the interests of its own staff and programmes.

The Area Desk is responsible for decisions involving attention and warning levels that may precede an evacuation, but consultation with the Security Advisor is always recommended.

Except where the sudden occurrence of events is accompanied by a communications blackout (cases where the Cesvi manager with most responsibility in loco decides), the staff in loco must always follow exclusively the indications agreed, as per the guidelines mentioned above.

Cesvi believes in the principle that since it is responsible for the safety of its staff, for protecting resources and for the success of its projects, any strategic decisions (such as those regarding the evacuation or otherwise of its staff, with the exception of the right of all operators to withdraw) are, in the final analysis, up to Cesvi.

[16] The pre-evacuation happens when the situation in a Country is deteriorating but there is still sufficient time to evacuate non-indispensable property and staff.

Administrative aspects and sensitive data

Money transfer and management

Movement and handling of money must be carried out in ways as set out in the Organisational Model.

Due to the security aspects involved, money management is an important activity.

Reliable banking services that manage money transfers without cash movements now exist in all countries. Nevertheless, if unavoidable project requirements make cash movements necessary, **specialised services** (companies specialised in money transfers, able to make good any possible loss of money by means of a formal guarantee) must be used, thereby avoiding the use of Cesvi staff or simple "specialised" civilians.

Amounts greater than those needed in the event of urgencies or evacuations may not be kept for day-to-day management of administrative activities in any single Cesvi office. In no case may cash amounts of more than €10.000[17] be kept in any currency at any single Cesvi base.

Two staff members should be involved in any procedures regarding the receipt, counting and protection of cash.

Whenever programmatic reasons make it necessary to work with sums of money or management procedures that don't match those provided for in the Policy and the administrative manual, the country Desk Officer must ask for an exception, providing a **Risk Assessment**.

Document and information protection

Documentation of an administrative and financial nature must be confidential and managed in an accurate and orderly fashion in order to prevent criminal actions.

Solely staff members whose jobs involve issues of an administrative and financial nature may access such documents.

The **correct use of information and its correct circulation** is an important part of any security measure. All information is by definition important in terms of security, and is therefore circulated solely to staff for whom it is intended. All staff members are responsible for the information they receive and forward. Any unnecessary circulation, whether internal or external to the NGO, must be avoided. Information concerning projects, security, administration, staff, context, property, resources and sites is always confidential and must be processed prudently to avoid its improper circulation.

Cesvi does not usually use encryption or cryptography in its communication methods.

All operators must take maximum care in making **appropriate use of the various communication means** (radio, email, Skype, etc.), thereby avoiding putting at risk their own security, that of colleagues or that of any other possibly interested parties.

Communications

Principles, means and methods

Without undermining the protection of documents and the confidentiality of information, **good communication** with colleagues and all the main interested parties **is indispensable for maintaining a high standard of security** in the NGO. All staff members are expected to contribute personally.

Unhealthy competition between members of the same team and between NGOs is a factor that considerably undermines the ability to respond to risks.

So as to prevent problematic situations, Cesvi promotes **transparent solutions of internal conflict** (see HR Policy) and intends to cooperate with other NGOs and humanitarian aid actors in maintaining relations of the highest possible standard.

[17] This should be seen as a maximum figure, which includes all resources necessary for a sudden evacuation. All efforts should be made to reduce the amount of cash in the offices.

Raising the overall quality of the system of relations between humanitarian aid actors can make a significant contribution to the maintenance of security.

The employment and correct use of modern communications equipment (radio, telephones etc.) is of great benefit to the management of security measures. Cesvi undertakes to pursue the highest standard possible in all its projects to guarantee the most efficient security management instruments through suitable tools and communication systems.

Debriefing and hand over

The contribution of all staff in the correct application and improvement of security procedures is essential for the application of this Policy. The participation of a numerous staff, like the one working for Cesvi, in this exchange and learning process is ensured by the following minimum methods:

- all expatriate staff must effect a hand-over with the Security Advisor, regarding security-related matters at regular intervals (during their meeting contacts at headquarters for example) and always at service termination;
- the Security Advisor will request and collect assessments and suggestions from all staff, both individually and collectively, during monitoring missions conducted in the field.

Transport

Car and motor vehicle use

Problems arising from traveling in motor vehicles are extremely important in terms of staff protection.

Unfortunately, there are frequent accidents. The following recommendations are intended to prevent or reduce their number.

No cars or motor vehicles that have not passed a regular road test in accordance with the laws of the relevant country may be used. All vehicles must be regularly insured in accordance with the regulations of the relevant country. Insurance premiums must be adjusted to guarantee cover of costs deriving from serious damages to third parties.

The use of automobiles exceeding ten years of age must be specifically authorised by the COO Chief of Operations.[18] In no case may economic considerations prevent the replacement of worn-out and inefficient motor vehicles with more efficient and modern ones.

In higher-risk countries[19], Cesvi allows solely suitably selected and prepared local drivers to **use cars and motor vehicles**. All staff must ensure that they know the highway code correctly, particularly the Head of Mission, who must terminate the contract of defaulters in the event of repeated acts of negligence, as per the procedures specified in the same contracts.

The Protection and Health Emergency document or the Security Plan expressly state the limits applied to staff when using cars and motor vehicles.

Motor cycles can be driven solely when wearing safety helmets.

The use of safety belts is obligatory on all vehicles that have them, unless in particular situations this would increase staff visibility and expose them to greater risk.

In all countries correct conduct when driving and other problems relating to driving motor vehicles (e.g. how to behave in road accidents) is dealt with in a specific, regular training session organised under the responsibility of the Head of Mission, or where envisaged, by the Country Security Manager.

[18] It should be remembered that in some countries the car fleet is exceptionally old and it is not easy to import new motor vehicles.
[19] Indicated in the country "traffic lights", with the red colour.

Even in the case of accidents caused by Cesvi staff, with valid third-party liability cover, the possibility of mitigating the consequences of damage by aiding the victims and their family members immediately, and also economically, should be assessed.

Flights

Cesvi does not allow its staff to use planes belonging to companies that are on the list of EU- banned airlines **(EU Black list)**.

The civil aviation authorities of EU member states are qualified to inspect aeroplanes of companies that fly to/from EU airports; given the casual nature of such random checks, it is not possible to examine all aeroplanes that land in all EU airports. Therefore, if a company is not included in the EU black list, this does not mean that it automatically meets the security measures currently in force.

Nevertheless the fact that a certain company figures in the list "does ring an alarm bell" with Cesvi.

Since checks outside Europe can sometimes be superficial or non-existent, the **reliability of any chosen airline** must therefore always be verified case by case, and the best choice made based on a set of information helpful in making the decision, by all actors in contact with Cesvi. All protection or security plans must contain any existing recommendations regarding this subject.

The use of non profit companies does not constitute a guarantee of a safer service. The reliability of these companies too must therefore be scrupulously assessed, by using the practical experience and information available in the relevant operational area.

The Security Advisor is on hand to advise staff on the most suitable choice.

Airport and customs regulations regarding flight security and goods transport must be scrupulously respected.[20]

Sites and premises selection

The **choice of the site** for opening an office or an operating base has important consequences for the overall security of a mission. Staff charged with the selection must therefore follow the **instructions contained in the security handbooks** referred to by Cesvi.

The Security Advisor is on hand for staff to make the best choice by taking all factors into account: the political and social context, official purpose of the premises, relations with the interested parties, the availability of services, accessibility, intrinsic protection factors, available budget, etc.

Photography and relations with the media

Cesvi staff should consider photography as an **operation to be planned in good time** just like any other documentation activity and/or relations with the media, since it is an indispensable and responsible way of sharing accountability on humanitarian aid and development cooperation activities with colleagues, donors and the wider public.

This activity should be carried out in respect of legislation on **protection of Privacy**. To illustrate the correct way of doing it Cesvi has prepared **particular documents on the use of images**[21] and on relationship with the mass media.[22]

Staff should never forget that important security factors come into play during communications with the media, so the contents of the above-mentioned documents must be closely followed.

Cesvi encourages journalists' and photographers' visits to its projects, seeing them as important in its wider responsibility of **accountability** towards donors and the public in general. However, during

[20] For example: do not carry packages without knowing their contents, prepare your own luggage personally, etc.
[21] See the following Cesvi's documents: *Policy on use of pictures of children and young people* and *Visibility and communication Handbook*.
[22] *Press Office Handbook.*

the mission planning stage those responsible must consult with the Area Desk and the Security Advisor, if necessary, to check that staff and Cesvi programme security will not suffer as a result of it.

Cesvi staff supervising photo-journalistic missions in loco must try to avoid situations that hinder Cesvi staff and projects.

Furthermore, staff must not put themselves or projects at risk by taking photographs or filming places where such activities are generally forbidden, such as airports, public buildings, political, religious and social meetings, military installations, etc.

Coordination

Joint security management

Coordination with other organisations is essential for the proper learning, management and development of security measures. Cesvi encourages its staff to take part in these networks.

Cesvi also favours the activities of networks or services promoted independently by NGOs. Cesvi generally uses various networks, concerning everyday management of security or to learning and exchange of general information. All Country Security Plans must clearly indicate any existing local security networks and the type of relations they have with Cesvi. They must also provide contingency measures in the event of the network ceasing operations for whatever reason.

EISF

The Cesvi Security Advisor is a member of **EISF**, the **European Interagency Security Forum**, which is made up of the security staff of European humanitarian agencies working internationally. The purpose of EISF is to facilitate collaboration and the exchange of information, to develop internal research and analysis, to provide accurate and empirical suggestions, etc.

EISF is a collaboration mechanism and not a service provider.

INSO

Cesvi recommends, in the countries where it is present, registration and use of the services of **INSO (International NGO Security Organization)**, a British non-profit organisation which works for the safety of humanitarian agencies in high risk situations. INSO supplies a range of free services to the agencies that register, among which are networking with other organisations, monitoring and real time information on incidents and crises underway, periodical analytical reports, statistical data on safety and their mapping, aid in handling crises, training and guidance for personnel.

Use of INSO services requires free registration on-site, which may be simplified with the help of Cesvi's headquarter.

ALLIANCE2015

Since the year 2000 the members of the **Alliance2015 consortium** have acquired considerable experience by working together in emergency and development situations. This has built up strong ties between the partners not only on the level of programmes, but also in the development of new working methods (mutual monitoring, training, support, advocacy, etc) which have led to the use of shared and harmonised operative approaches and tools.

Within Alliance2015 there is a **work team made up of the Security Officers** at a global level, who work together on information exchange and who meet up periodically with shared programmes.

Although to date no official common protocol exists for security management Cesvi recommends, where possible in the single countries, collaboration with other partners of the consortium in order to increase the quantity and quality of safety information and its exchange, the awareness of existing risks and the circulation and promotion of good practice and lessons learnt.

Italian Foreign Office Crisis Unit

The **Italian Foreign Office Crisis Unit** is the Ministerial body that aids Italian citizens abroad. Similar services exist in various countries to deal with crises or emergencies abroad. These services are mainly interlinked with each other and are in contact with those of Embassies.

One of the Crisis Unit activities is monitoring the presence of Italians in the world via the web-site: **www.dovesiamonelmondo.it**

All Cesvi expatriate staff are registered on the site by the HR team. The data is treated according to the regulations regarding the processing of personal data.[23] The Crisis Unit is responsible for the management of the site.

In emergencies Cesvi can contact the Crisis Unit in order to protect its staff.

However, Cesvi makes an independent assessment of any information provided by the Foreign Office Crisis Unit, the Embassy network and other similar services of other Countries, and is not obliged to follow them in the case of its own staff.

The Security Advisor is the person in charge of interacting with the Crisis Unit. In serious situations the Cesvi Crisis Team may interact with the Foreign Office Crisis Unit.

United Nations Agencies

Cesvi works with **UN agencies** in the implementation of humanitarian aid or development cooperation programmes.

The assessment of the UN's position and security measures in the face of persistent risks or threats in any given context is of great importance. This is performed in single countries by the Country Security Manager, the Head of Mission, and on a global level by the Security Advisor. Cesvi is aware that interacting with such agencies is often of fundamental importance for a profitable and continual risk analysis of the single contexts where it operates. Cesvi points out that since these Agencies have no specific responsibility towards NGO staff (sometimes also for projects co-financed with UN resources), Cesvi's primary responsibility is to the security of its own staff.

Civil and military relations

Increasingly frequently the NGO finds itself operating in **situations where armed forces are active**, legitimised or otherwise, by a State recognised by the United Nations. Then there are situations where armed forces are involved in peacekeeping or peace-enforcing operations, with or without an explicit mandate from the United Nations.

The question of civilian and military relations in a humanitarian aid context is therefore a complex one in continual evolution.

The development of the repercussions on civil and military relations (CMR), the coordination, the dialogue or the co-existence of military forces and NGOs in situations where Cesvi operates is being followed carefully via the networks of which it is a member (e.g. VOICE).[24]

Cesvi has learned how **civilian-military coordination** is useful for the success of humanitarian aid actions on various occasions (for example when the military forces had a clear mandate, where there was wide-spread acceptance of the same by part of the population of the country where operations were being carried out, when the military forces respected the role and the "humanitarian space" where NGOs were operating).

On these occasions the logistic support (transport, air flights, communications) that the military forces are able to offer can be useful.

[23] *Programmatic Security Document (Legislative Decree 196/2003).* It is better known *as* the *privacy document.*
[24] www.ngovoice.org.

Each situation is different from all others; so before any form of collaborative task is started, attention must be paid to any risks that Cesvi staff, the programme recipients and other NGOs might run and to the risk of compromising Cesvi's neutral, independent and impartial position.

The analysis takes into account the attitude of the "humanitarian community " (NGOs, United Nations Agencies, International Red Cross) in the area in question.

For this reason Cesvi invites its staff to assume a **cooperative and positive attitude** towards any possible synergies that might spring up within any particular context with armed forces legitimised by the United Nations, but not to underestimate the consequences.

The independence of staff in the field in assessing situations being understood, the Security Advisor must be consulted for guidance in advance of any situation that requires conducting regular relations with military forces.

All formal agreements require the authorisation of the COO Chief of Operations.

Relations with local authorities

Staff, visitors and anyone frequenting premises or activities falling under Cesvi's responsibility must respect local laws regarding[25] trade, export and import of goods and money, access to determined areas, buildings, visas, access, residence and transit permits, labour laws, highway codes etc. Any unclear situation must be discussed with the contact person.

In addition to being a general principle of Cesvi's mission, **respect for the laws and local customs** is of great importance in developing consensus for the NGO's operations and, in the last analysis, also for the security of its staff (of whatever nationality) as well as for the success of the programmes.

Cesvi will therefore check how regular registration can be obtained for the NGO in the country where it will operate before the start of the mission if possible and will complete it as soon as possible.

All staff will have **visas** and **work permits** in accordance with the aims of the missions entrusted to them.[26]

Labour and business laws etc. in force in various countries which are also applicable to NGOs, shall be examined in depth by the staff in charge of Coordination or Administration so that the NGO's affairs will be managed in accordance with local laws.

Information regarding the NGO's activities will be communicated to the relevant local authorities via reports, meetings, etc. informally and will be aimed at obtaining approval for operations performed, in order to reinforce the authorities' support for future programmes. This all has important consequences in terms of the security and protection of staff and the NGO's programmes.

Should problems arise with local authorities, the Core Team of the internal Crisis Unit and the Crisis Committee "Relations with mass media in crisis situations" are to be informed.

Visitors, family members, accompanying persons

All visitors to Cesvi Projects are advised to study the security measures contained in this Policy, even when no formal contract exists between the visitor and Cesvi.

All offices abroad have a notice in the entrance recalling that "Correct observance of the rules that Cesvi has adopted for the security of its staff and visitors is a guarantee of protection for everyone. Anyone requiring further information regarding the security Policy existing at this base should refer to the... Name of the Country Security Manager or of the 'Head of Mission, Date and signature of the Head of Mission."

Cesvi staff members accompanying or organising the visitors' mission are responsible for informing them of the existing security measures. Cesvi staff members are responsible for informing their own visiting family members of the contents of the Cesvi security Policy and other related documents. Accompanying persons must also prevent, deal with and resolve any form of visitors' conduct that could put Cesvi and its staff at risk in any way.

[25] This list is merely an example and is no way comprehensive.
[26] The Legal and Organization Advisor and the Area Desk together with the HR Team are responsible for registrations, visas, work permits etc.

FINANCING OF SECURITY MEASURES

The putting into practice of an effective framework of risk management for security purposes calls for an adequate commitment of **human and financial resources**, which must be provided for assigning security positions, purchasing materials and equipments and for training personnel.

Most Donors recognise that guaranteeing the safety of personnel is essential for a programme to be correctly completed and are consequently more and more willing to finance the costs.

It is the Area Desk's responsibility to ensure that the project proposals always include the **costs related to security management**, according to the risk level in the countries concerned. Cesvi contributes with its own resources to the costs related to the Security Advisor's training and position.

The Security Advisor supports staff in accessing donor resources to cover security costs and is available to staff during the preparation of the project budget section regarding security costs.

BENCHMARK

Cesvi seeks to offer its staff the best possible system of security management measures and procedures. The last ten years have seen a **highly positive development in security management practices** among NGOs. This process is still underway and the positive competition between NGOs continues to raise the quality of the services offered.

Cesvi believes that this process contributes to the overall **credibility** and **reliability** of the NGOs.

Cesvi intends to contribute to this process by sharing its own security procedures and measures with NGOs willing to do the same, with a view to working together for raising the quality of the work performed by NGOs.

POLICY APPROVAL, MONITORING AND REVIEWING METHODS

The present Policy, **approved on 20th December 2017 by the Board**, the only body with the power to authorise revisions, brings up to date the preceding version of 20th April 2009.

The Security Advisor may use participatory consultation methods to check on how all or some parts of the Policy are being applied. The results will be found in the Annual Security Report.

SUGGESTIONS

The people designated to receive suggestions from the Desk Officers, concerning the contents of the Policy, exclusively through their Unit Directors, are the CEO-GM, the COO and the Security Advisor.

ATTACHMENTS

Special part of the Organisational Model relating to health and safety in the workplace

Incident/accident report form

The collection of data relating to accidents is an important activity for identifying any gaps and for monitoring how security procedures are applied in the field. This procedure is also compulsory in the events of incidents causing traumas to any kind of staff.

Hereunder a model form for data collection is proposed.

It should be filled in with the following information:

- All events, even simple threats not followed through or events that have caused damages to objects, persons, assets or resources must be included. Violent actions and serious illnesses must also be included. Attempted and unrealised theft must also be included, therefore.

- No distinction must be made between events involving local staff or expatriate staff: both categories are equally important for Cesvi.

- Also events involving other NGOs, especially NGOs that have a formalised relationship with Cesvi: partners, Alliance2015 NGOs etc.

- Suspensions of the normal continuation of programmes caused by incidents or the threat of incidents.

- Accidents occurring to the main actors (e.g. UN, National Development Cooperations, etc.) in the same area where Cesvi staff operate.

Please Note: Italian law requires any accident occurring to staff with contracts registered in Italy to be reported. It must be reported to the INAIL offices within 48 hours of the event that caused the suspension of labour for at least three days. The lack of report is a serious contractual infraction.
Accidents are reported on the following form and sent to the Security Advisor and Personnel Administrator. Contact details for the latter are supplied together with the insurance policy.

Incident/accident data form contents:

Prepared by

Position

Date

Date of event

Time of event

Exact location

Description (persons involved, causes, consequences)

Any actions undertaken following the event

Suggestions and comments

Early warning

This form provides some general indications when having to report an emergency situation.

The Security Advisor, or alternatively the COO Chief of Operations, is the person in charge of receiving any early warnings. Their contact numbers are normally given to all staff before the start of a mission and are included in the contact lists available to staff in the field.

Other channels must be activated locally:

- the Country Security Manager, where existing

- the Head of Mission

- relevant Embassies

- the Area Desk

- the medical evacuation system, when necessary

- the Foreign Office Crisis Unit (in imminent life-threatening situations)

- any other contact defined as such in the event of emergency (e.g. local Authorities, local Police, etc.) included in the following documents: Health Protection and Emergency Plan and Security Plan

Country security plan contents

A country security Plan always contains an in-depth study of the following aspects, but must never exceed twenty pages (excluding attachments):

- Title: the areas in question

- Profile of NGO in the country: aims, projects, counterparts, visibility, staff and responsibility etc.

- What to do before arriving in the country.

- What to do as soon as you arrive in the country.

- Localisation and description of operating areas: offices, staff accommodation, roads, etc.

- General rules of conduct: dress, laws and local customs, personal equipment, health precautions, places you can visit or should avoid, curfew, conduct in critical situations (e.g. intimidation, aggression, etc.), visitors, etc.

- Rules relating to driving motor vehicles and transport (flights, road blocks, night-time travel etc. and relative to accidents).

- Any general information about the presence of mines or unexploded bombs.

- Communications management rules

- Rules for visits in the field.

- Coordination with other actors in the field.

- Communication means and methods: radio, early warning systems etc.

- Health problems, emergency and medical evacuation.

Administrative problems:

- Everyday Security Management: guards, R&R, etc.
- Notes and recommendations regarding special operational areas.
- Evacuation plans for each operational base.
- What to do in the event of closing a mission.
- Any other useful information.

Attachments:
- Description of the country context and main existing risks;
- Contact list (staff, NGO, public bodies, police, international organisations, etc.);
- Health centre list;
- MAPs
- Acronyms

Annual security report contents

Includes the following:

- Security Advisor's activities (Recommendations, Missions, Valuations, Networking, etc.);
- NGO security management: problems arising;
- Security traffic light;
- Accidents and assessment;
- Training;
- Draft Security Plans;
- Activities aimed at preserving the "humanitarian space";
- Future work ideas;
- Final budget and estimate.

APPENDIX

Security Management

Cesvi's Policy

The application of security measures, in Italy and in the field,follows the managerial lines of Cesvi's operations structure.

In the headquarters the CEO-GM is directly responsible for the application of security measures. Abroad, the application of security measures follows the operations line from the CEO to the Project Manager to the Area Desk to, lastly, the Head of Mission (HoM)

In the higher risk countries the specific figure of Country Security Manager (or Officer) is **provided for**.[27]

The Security Advisor holds a position, in relation to the **operations** structure, of training, encouragement, orientation and verification.

Different Security Management Models

1.Operations Line Model (Mainstreaming): The responsibility for security management follows that of the **operations line**, including the administrative, RU and Programming staff.

Advantages	Disadvantages
• Knowledge and understanding of the programme; • Possibility of including and optimizing security in all the planning activities (finance, logistics, HR); • Ideal for consensus with the communities (as mitigation strategy); • More rational in the definition of security budgets; • Less risk of internal conflicts at the decisional level;	• Time consuming (according to the country context); • More difficult to find staff with dual professional training; • Lower crisis management ability; • Requires a rooted security culture in the NGO; • Optional if the function is to be *ad personam* or to Reference Terms;

[27] The role of Country Security Manager is, usually, non compatible with that of Head of Mission (if not for brief periods), in order to keep distinct the responsibilities of control, support, advice, training and representation on security matters from other management or representational duties.

2. The Security Specialist Model (Pure Security Officer): This model is generally used in high risk countries (intervention areas); it involves one or more security specialists allocated to the HQ and the general and peripheral offices of the mission; their authority is subordinate to that of the Head of Mission.

Advantages	Disadvantages
• Higher technical competence; • Higher crisis management capacity; • Easier to fit into the organisational chart; • Completely dedicated to security; • Helps increase the security culture;	• Costly; • Difficulty in hiring; • Perception of security as a separate sector; • More bureaucracy; • Less knowledge and understanding of the programme; • Prone to favour protection/deterrence rather than consensus; • Higher risk of internal decision making disputes (HoM);

3. Security Consultant Model (Mixed): responsibility for security is assigned to operational management with the back up of an internal or external consultant with no direct managerial authority.

Advantages	Disadvantages
• Inexpensive, easy and quick to add to a pre-existent organization; • Good technical ability; • Good crisis management ability; • Totally dedicated to security; • Effective for those NGOs with little security culture; • Contribuisce ad aumentare la cultura della sicurezza;	No field operation

Job Description

JD Security Advisor

The Cesvi Security Advisor is responsible for staff security abroad. The **Security Advisor**:

- informs, supports, directs and draws conclusions from the risk analysis process;
- develops, promotes and monitors the application of the measures included in the Policy and related documents (Protection and Health Emergency Plans, Country Security Plans, etc.);
- advises any other official (President, H&S Manager/CEO-GM, COO Chief of Operations, Head of Mission, Country Security Manager, staff) on questions concerning risks, protection and security of staff abroad;

- supervises and implements the Security Training Plan whenever that is possible, promotes staff training and is directly responsible for that of the Country Security Manager;
- offers advice to all staff members on questions concerning security;
- checks that security measures correspond to those of this Policy;
- suggests changes to this Policy and to security measures;
- up-dates and analyses the incident/accident data base;
- drafts the Annual Security Report.

The Security Manager has an annual budget for the above activities.

Desk Officer's JD

In carrying out his job the **Desk Officer**:

- is responsible for the application of all security measures (drawn up by the Security Manager in the specific country and reviewed by the security Advisor at HQ) for the countries he/she is assigned to;
- ensures from time to time that the security measures in those countries (S&S plan, Country Traffic Light, Monthly Report, Incident Report, etc.) are updated both to meet fixed deadlines and in exceptional cases according to the country context;
- is responsible for the choice of organisational model for security management for his/her countries (Pure Security, Mainstreaming, Mixed)
- is responsible for defining the organisation of security staff in the country, on which will depend the communications and the hierarchical and functional relationships between staff with security roles at head office and in the field;
- is responsible for periodical evaluation of the skills, the commitment and the results achieved by staff with security roles;
- is responsible for guaranteeing the annual allocation of funds for security;
- is responsible for communicating to the HQ Security Advisor any changes in the organisational chart of staff with security roles:
- supports the Crisis Management team in the following tasks (following the specific guidelines):
- providing direct assistance to overseas offices;
- assisting the CMT in initial contacts with the competent authorities;
- providing contextual information;
- communicating with the local Incident Management Team.

Head of Mission's JD

The JD is the same as that of the Desk Officer, but carried out at the country level in coordination with the Desk Officer and the Security Advisor.

Country Security Manager's JD

The CSM function may be assigned as a single role to a dedicated person, or as an added task to someone with another main responsibility, or distributed among various people with other main jobs.

In carrying out his/her role the **Country Security Manager** is responsible for:

i General Security

- has the responsibility for the security of local and international staff, for Cesvi's assets, resources and documents (including administrative ones) used in the country, through the application of the instructions and the respect of the principles contained in the Security Policy, in the Country security Plan and in the other reference documents related to security;
- promoting staff knowledge of the ECHO Security Manual and internal documents relating to security (Cesvi Policy, Cesvi Security Handbook, Country Security Plan, etc.) and those related to the context analysis and residual risks in terms of Due Diligence and security circulars;
- promoting the application and the updating of in force, with particular attention to staff movement, to protection of work sites, to communication and evacuation routes including all related bureaucratic aspects (issue of visas, flights etc.);
- has the responsibility for reviewing the security documentation, adapting the contents to the specific local context;
- guarantees the writing of reports and the processing of information on security matters addressed to the Project Manager and Head of Mission for the drawing up of accounts due to third parties (backers, head office, Contact, government bodies in the host country etc.);
- monitors the daily and periodic information in the *Security Bulletins* and mass media, in order to identify the main facts and emerging trends for suitable distribution and communication to appropriate recipients
- renders official and files the decisions and the key changes concerning security;
- observes, based on a continuing analysis of the context in the Country/Area of intervention, the existence of possible imminent threats or emerging trends concerning security, and gives advice and support to mitigate possible consequences.

ii Training

- trains expatriate and national staff on security matters and ensures periodic updating with one-to-one or group meetings:
- is responsible for holding introductory briefing on security for HQ staff on mission, for employees and those collaborating on projects, for consultants on brief or long term missions, for the families of staff duly authorised to accompany or to visit the mission, for authorised visitors, for the volunteers in the field, for interns and every other person with a formalised and direct partnership with the NGO;
- identifies and facilitates training of staff, within the limits of available resources, through outsourced training.

iii Logistic activities

- verifies and ensures that, relative to security, the logistics of the ongoing projects meet the regulations in force in the country, the rules established by the financiers, and the organisational procedures (Policy, Security Manual, Country Security Plan etc.);
- undertakes missions, in the Country or the Area, to verify that the envisaged security activities are put into practice as well as those necessary for the support of exploratory or emergency missions;
- ensures the efficient organisation of the office and an orderly filing (both paperwork and IT) of the security documentation;
- guarantees that the security means, equipment and logistic apparatus for security, in line with the final objectives, are inventoried and in working order;

- ensures the correct usage and maintenance of all the security apparatus provided and ensures the necessary training for a safe and correct usage by the staff.

iv Identification of new proposals

- contributes to drawing up, for those aspects in his/her remit, the paragraphs concerning security and the conflict analysis in new project proposals;
- guarantees the necessary support on security matters to the missions for feasibility studies in the Country and the Area he/she covers.

v Administrative and Legal

- collaborates with the administrator for the correct and timely attribution of security expenses under his/her remit;
- assures particular care in the conservation and handling of confidential information which comes into his/her possession for the role he covers;
- guarantees the administrative management of the budget line for security in his/her remit and of any related problems that may arise, keeping the Head of Mission informed;
- collaborates in the recruitment of local staff, following the criteria of the internal rules, verifying – only for the security aspects – the moral and professional eligibility to carry out the work, and defining the specific tasks;
- for staff with contracts under Italian law (expats) he works in coordination with the Head of Mission and the Human Resources administrator of the HQ, concerning communications to them, including timely notification of information for the security circular.
- guarantees the collection and conservation of all the documentation required concerning information to staff, for legal and auditing purposes.

vi Visibility and Communication Activities

- for security purposes and respecting the security profile in force in the country, oversees the use of the logo and visibility material of Cesvi, following the Visibility and Communications guidelines;
- takes part, for the security aspects, in organising of internal units' communication and fund raising missions and those of journalists, photographers and press officers of other organisations.

vii Crisis Management Plan

Completes the Incident Management team at the country level in respect of the specific guidelines; the responsibilities of the Head of Mission will concern in particular:

- management of local level crises;
- management of the security of all staff;
- management of necessary evacuations and transfers;
- coordination of communication channels with the families of national and international employees;
- keeping of regular contacts with CMT
- updating CMT on the situation in the field, with accurate information;

- creation and updating of a register of all the aspects of the crisis;
- coordinating role with:
    - *national authorities concerning the resolution of the incident*
    - *other organisations in the country as requested;*
    - *the local offices and embassies of key donors*
- management, in agreement with the CMT, of communications with the mass media
- ensuring operational continuity in cases of prolonged crises.

Field Security Focal Point's JD

- is responsible for the application of the instructions of the Security Policy, the Country Security Plan and of the other documents relating to security, limited to one office or one specific area of competence (remit area):
- guarantees staff coordination of his/her assigned office or base concerning respect of the security rules;
- is responsible for induction, training etc. of the staff working in his/her assigned office or base;
- within his/her area of authority he/she is responsible for the collection and timely transmission of information, from primary and secondary source, in order to keep the whole security context up to date;
- is responsible for promptly informing the Security Manager and Head of Mission (or other figure indicated in the communication tree) in case of imminent dangers that might require the temporary suspension of the field activities.