CILC
Center for International Legal Cooperation

Travel Security Policy

August 2017

Table of content

1. Introduction 2
2. Fundamental Principles of Travel Security 3
3. Scope of the CILC Travel Security Policy 4
4. Roles and Responsibilities 5
5. Risk Classification / Assessment 6
6. Business Travel Insurance 7
7. Travel Preparation 8
8. Security during stay abroad 9
9. Monitoring 10
10. Crisis Management 11
11. Policy Review 12
Annex A: Emergency Contact Information Sheet 13
Annex B: Basic Travel Security Rules 14
Annex C: Incident Reporting Format 17
Annex D: Crisis Protocol 18
Appendix D1 – CMT members and contact details 20
Appendix D2 – Crisis Room layout 21
Appendix D3 – Logbook 22
Appendix D4 – Agenda first meeting 23
Appendix D5 – Agenda second meeting 24
Appendix D6 – Guidelines for the untrained negotiator 25

1. Introduction

The Center for International Legal Cooperation (CILC) is an independent Dutch non-profit organisation founded in 1985. CILC is a foundation according to Dutch Law, with a mission to provide expertise to developing countries and countries in transition engaged in legal and judicial reform.

In order to implement this mission, CILC employees and contracted experts travel to and work on short- and long-term missions in various locations around the world. CILC is aware that travelling to certain locations comes with personal risks towards employees and experts, as well as with financial risks for the organisation. As a matter of duty of care, the primary objective of this Travel Security Policy is to minimise the risk to individual employees and contracted experts during such travel and while their stay abroad. Secondary objectives are the enablement of duty trips and the protection of the reputation of CILC.

The aim of the present document is to outline a number of principles and practical arrangements related to security policy for business travel and living abroad of permanent CILC staff[1], as well as CILC contracted international short-term and long-term experts[2].

[1] *The Travel Security Policy only applies to business related travel.*

[2] *In case these experts are not independent experts and thus employees of other sub-contracted organisations and institutions, relevant Travel Security Policy documents of these organisations and institutions apply to them as well.*

2. Fundamental Principles of Travel Security

Duty of Care

Article 7:658 of the Dutch Civil Code forms the legal basis for the employer's liability. It states that the employer is liable for damage that employees sustain while doing their job. The article is based on the principle that an employer is liable for such damage unless it can show that it has fulfilled its duty of care or that the damage is the result of intent or wilful recklessness on the part of the employee. In addition, an employee can hold his or her employer liable on the grounds of good employment practices as laid down in Article 7:611 of the Dutch Civil Code.

Central to CILC's Duty of Care is the preparation of staff through training, and the regular review of the organisational capacity to respond to critical incidents. CILC views Duty of Care as a legal and moral obligation that ensures the safety of all people falling within its management control. CILC will not consciously expose anyone to unacceptable levels of risk. CILC exercises due diligence to make sure no one suffers avoidable mental or physical harm.

Elements of Duty of Care

In order to implement this view on travel security, CILC works to:

- conduct systematic assessments of risks / have an up-to-date picture about potential risks;
- prepare staff and contract experts;
- strengthen the accountability of the organisation in security issues.

Fundamental principles of CILC Travel Security Policy

There are a number of fundamental principles that guide the CILC Travel Security Policy:

1. For CILC, life precedes material and therefore no CILC employee or CILC contracted expert should endanger his/her own life, or the life of others, whilst attempting to protect material interests.
2. Specific risks of a destination should be assessed in advance and adequate measures need to be in place in case of necessity. Otherwise the travel should not be undertaken.
3. Employees and contracted experts are always informed beforehand of and prepared for the level of risk of any given mission and by accepting the mission they accept the risk. However, unforeseen developments may occur and therefore every employee and contracted expert has the right to request to suspend activities, to withdraw and/or to leave the area. Such requests will be discussed by the involved managers with the Board and granted if deemed reasonable.

3. Scope of the CILC Travel Security Policy

The scope of the CILC Travel Security Policy is to regulate the security issues of project and other business related missions conducted by CILC staff and/or CILC contracted experts, as well as to regulate security issues related to the deployment of CILC staff and CILC contracted long-term experts abroad[3]. This policy also applies to independent, self-employed contractors hired by CILC for work within CILC projects.

Sub-contracting companies are responsible for the security of their employees. In combined activities however, an agreement can be made with regards to procedural measures in order to ensure consistency. In case another party organizes the business travel for CILC staff or CILC contracted experts, the same security principles, as outlined in the CILC Travel Security Policy, should apply. This is to be checked in advance by the respective project officer or (junior) project manager.

This policy applies 24 hours a day 7 days a week for the complete itinerary of the traveller, including parts of international travel that take place in the Netherlands. This policy does not apply for activities that place on non-working days/pre-agreed moments of leave. However, the CILC employee and the CILC contracted expert are at all times expected to avoid high risk areas, not to undertake dangerous activities that fall outside the scope of the CILC travel insurance and obey local laws and regulations.

Core themes

Core themes of the CILC Travel Security Policy are:

1. *Risk categorisation*: within CILC, all destinations are categorised by a risk profile in order to determine proportional and relevant measures;
2. *Preparation*: CILC will enable all employees and experts to prepare themselves by means of adequate instructions regarding travel safety and security;
3. *Travel monitoring*: all travel itineraries that fall in the scope of this policy are kept centrally and are easily accessible in case of necessity. Travels outside the scope of this policy can be shared on a voluntary basis. The itineraries, contact, HR and personal details are accessible to the Board in case of emergencies;
4. *Emergency protocol*: CILC will exercise and maintain a protocol for critical incidents or emergencies.

[3] *The CILC Travel Security Policy defines 'abroad' as located outside of the country of residence/origin.*

4. Roles and Responsibilities

Roles

In the Travel Security Policy one has to divide three levels of roles and responsibilities.

First of all, there is an *individual responsibility of each traveller* (CILC staff or CILC contracted expert).

Secondly, in the implementation of the travel security measures, there is a role for the respective CILC project staff in charge of / organising the travel of the CILC contracted experts or the CILC staff (*travel security officers*).

Thirdly and finally, at the level of defining and monitoring the implementation of the measures under the Travel Security Policy there is a role for the *Board of CILC*.

The *travel security officers* (project officers or junior project managers making the logistical arrangements for the travel of CILC contract experts and CILC staff) have the following tasks:

- have the overview of all business travel locations and travel duration of employees and CILC contracted experts as well as overview of CILC contracted long-term international staff; and
- be the first contact point for reporting by CILC contracted experts and CILC staff for any issues during business trips.

In case a travel security officer will be on a business trip himself/herself, the mentioned tasks should be delegated to a replacement.

Business travel itinerary e-mail address

For all business trips, the e-mails with the travel itinerary should also be send to a separate e-mail address: travel@cilc.nl. In this e-mail box all business trip itineraries will be stored. The travel security officers and the Board should have access to this account. This box (which is just an in-box) will be periodically cleaned.

Immediate access to certain information

When a situation occurs abroad where CILC staff or CILC contracted experts are located, the travel security officers should be able to provide at short notice the following information:

- Place where the CILC staff or CILC contracted experts are located;
- How CILC staff and CILC contracted experts can be reached, directly or indirectly (local office, local counterpart);
- Who can be contacted as the CILC staff's or CILC contracted experts' contacted person in the Netherlands/country of residence.

The CILC Board will be responsible for monitoring the implementation of the Travel Security Policy and its regular review.

5. Risk Classification / Assessment

Risk category

There are three risk categories (Low, Medium, High) of travel destinations within CILC's Travel Security Policy. Travelling to a destination within a certain risk category has consequences for the responsibilities and security measures for the involved employee. Countries are primarily categorised on the basis of travel advice by the Dutch Ministry of Foreign Affairs (www.nederlandwereldwijd.nl/reizen/reisadviezen), which has 4 different ratings, based on colour coding. In case of any uncertainty about the advice of the Netherlands Ministry of Foreign Affairs or the need for a double check, alternative sources are: www.gov.uk/foreign-travel-advice and www.auswaertiges-amt.de/DE/Laenderinformationen/01-Reisewarnungen or the country reports of the AIG Business Travel Insurance: https://travelguard.secure.force.com/TravelAssistance/TGHomePage?PL=AIG+Netherlands.

Category	Dutch MoFA rating
Low	Yellow, Green
Medium	Orange
High	Red

In principle, CILC does not carry out missions to destinations in a 'red' rating.
CILC reserves the right to place destinations in other categories than initially would be the case, based on the table above. The CILC Board can place countries in a higher category, if deemed necessary. In order to place a country in a lower category, a full analysis is needed, including:

- The full text of the travel advise from the Dutch Ministry of Foreign Affairs and/or alternative sources;
- Advice from a local counterpart;
- Advice from the involved CILC project manager(s);
- An overview of the specific risks that CILC will run, in terms of impact, probability and proposed measures.

6. Business Travel Insurance

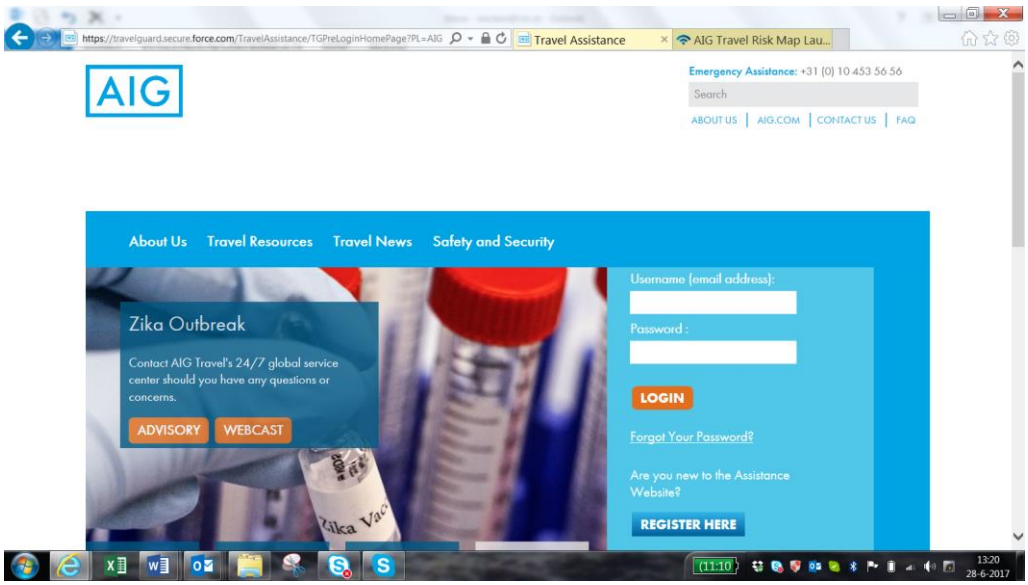
CILC has a *travel insurance for business travel* for every CILC staff and international expert travelling under CILC responsibility: the "AIG Travel Guard Business Travel Insurance" (policy number: 60.10.4375), also called 'Chartis Business Travel Insurance'. The broker for this insurance is 'Jonker-Schotte Adviesgroep'. Contact person: Marco Scheffers.

The insurance has a world-wide 24/7 emergency number: + 31(0)104535656, which together with the Name and Policy Number of the insurance is to be mentioned in Expert Letters. CILC staff has a Chartis Emergency Assistance Card with the same information mentioned: Name, Policy Number and the Emergency Phone Number.

The insurance covers the expenses in the case of:

- personal accident;
- medical expenses and assistance;
- loss or damage of personal belongings and business equipment;
- cancellation, interruption, delay and replacement of the travel;
- legal assistance;
- personal liability;
- hijack, kidnap, unlawful detention; and
- political evacuation and crisis/disaster evacuation.

Though the website of the AIG Business travel Insurance (login required) https://travelguard.secure.force.com/TravelAssistance/TGHomePage?PL=AIG+Netherlands useful information, like security alerts, country reports, up-to-date health issues can be found, including on-line security training.



Moreover, CILC also has a *disability insurance and a liability insurance for its permanent staff*.

Long-term experts, including locally contracted experts should also be obliged to have a *medical insurance* that covers medical costs abroad. A copy of the medical insurance card for international and national long-term experts should be attached to the respective Assignment Agreement/Consultancy Contract.

7. Travel Preparation

Good preparation

For safe business travel a good preparation is essential and in case this is necessary, security conditions and measures should be in place.

The basis of good preparation within CILC is the fact that travellers themselves are responsible for gathering information, informing the organisation, comply to this policy and to apply common sense.

For medium risk destinations, destination specific advice and experience is collected by the respective project manager and shared with the traveller. This can include a list of preferred suppliers for accommodation and transport, meet and greet procedure at the airport, medical facilities, advised vaccinations and an overview of cultural and local sensitivities that might apply in that country.

In case of high risk destinations, CILC will not undertake travels to these destinations.

New CILC staff members, who have not had any travel security training, will be obliged to attend the Expat Preventive travel security training or a similar training offered by another company. A refreshing course on travel security will be offered to CILC staff every five years.

Accessible and up-to-date contact information

A key element of the travel security policy will be that information about the traveller and his/her relatives/contact persons at home are accessible. For this purpose the traveller will be asked to fill in a form with his/her contact details and those of his/her contact persons in the Netherlands/home country. For frequent travellers it will be sufficient to fill in this form once. Only in case of changes, the form will need to be updated. The form with Emergency Contact Information is attached as annex A to the present document.

Basic rules and checklist

A list of issues related to Basic Travel Security Rules for preparation of the travel and during the travel is attached as Annex B. It is advised to attach this list to expert letters / contracts.

8. Security during stay abroad

For the permanent CILC staff as well as the contracted experts it is essential to:

- Know the location of the nearest Dutch consulate or embassy or the Embassy/consulate of the expert's country of residence, as well as their contact information;
- Be familiarised with the national and local laws. Keep in mind that some customs may seem optional, but if not observed may cause problems;
- An understanding of how the health insurance covers the stay abroad.

Indicate:

- Standard of local medical care;
- Risk of serious infectious diseases.

Medical risk can vary within country:

- Major cities may have lower risk;
- Remote areas may have higher risk.

Risk assessment depends on:

- Age;
- Gender/pregnancy;
- Previous medical issues;
- Current physical and mental health status;
- Immunisation status;
- Use of medications; and
- Behavioural patterns.
- Category of the travel destination (low vs. medium risk)

A list of issues related to Basic Travel Security Rules for preparation of the travel and during the travel is attached as Annex B. It is advised to attach this list to expert letters / contracts.

9. Monitoring

Accessible information about itineraries and contact data

CILC maintains an overview of the whereabouts of (traveling) employees/contracted experts deployed abroad and their personal contact, as well as their contact persons in the Netherlands/home country in order to better respond to emergencies or changing circumstances. Compliance to travel monitoring applies 24/7 and the complete itinerary in case of a duty trip. For employees stationed in the Netherlands, this travel information is collected by the project manager and stored at a central location, easily accessible in case of necessity.

As every traveller is notified about his/her itinerary, a copy of the itinerary will be send to a separate e-mail box that is just to store all business travel itineraries: travel@cilc.nl. This e-mail box is emptied regularly.

Incidents reporting

All security incidents or near-incidents should be reported by the employee, the contracted expert or their manager to the Board. The Board will then discuss on the follow up and actions needed. The traveller or colleague reports at least the following information to the Board:

- Who (is involved? CILC travellers or others);
- What (has happened, what are the actions so far?);
- Where (did the incident occur?)
- When (did the incident happen and is the situation still ongoing?
- How was the incident addressed?

A format for the Incident Reporting is attached as Annex C.

CILC staff reporting during business trips

In order to keep track of CILC permanent staff during missions abroad, it is advised to introduce a reporting procedure under which the respective CILC staff member report (SMS, instant message, phone call, e-mail) to the Board upon arrival in the country of destination and upon return in the Netherlands.

10. Crisis Management

Emergency Number

In case of any incident during a business trip, CILC staff or contract experts can contact the alarm centre of "AIG Travel Guard Business Travel Insurance" (policy number: 60.10.4375), also called 'Chartis Business Travel Insurance'. The insurance has a world-wide 24/7 emergency number: + 31(0)104535656, which together with the Name and Policy Number of the insurance is mentioned in Expert Letters.

CILC staff has a Chartis Emergency Assistance Card with the same information mentioned: Name, Policy Number and the Emergency Phone Number.

Through a Dutch 010 number, the traveller will be connected to the nearest AIG Alarm Center to the location the traveller. The traveller just needs to mention:

- Name;
- Location;
- Condition and query;
- Policy Number;
- Telephone number to contact traveller.

The first attention of the Alarm Centrale will go to the traveller. Once all arrangements for the traveller are made, the Alarm Centrale directly or indirectly informs the CILC Board / management.

Crisis Protocol

In case of a major incident a crisis team, with potential participation of outside advisors, will be set up. For such a situation the Crisis Protocol (Annex D) will come into force.

Informing the CILC Supervisory Committee

In case of a life-threatening situation and possible outside attention to this situation, the CILC Board will also notify the members of CILC's Supervisory Committee.

11. Policy Review

This policy is reviewed on an annual basis by the Board. The basis of the review is:

- Experiences so far with the Travel Security Policy and the related processes;
- Incidents that might have occurred; and
- CILC international's response to those incidents and the functioning of the related emergency protocols.

Annexes:

- Annex A: Emergency Contact Information Sheet
- Annex B: Basic Travel Security Rules (for preparation and during business trips)
- Annex C: Incident Reporting Format
- Annex D: Crisis Protocol

Annex A: Emergency Contact Information Sheet

Employee/Expert Information	
First Name	Fill in…
Last Name	
Mobile phone number	
E-mail address	
Emergency Contact	
Primary Contact Name	
Relationship to Employee/Expert	
Emergency Home Address	*Country* *Address 1* *Address 2* *Address 3* *City* *County*
Home Phone	
Primary Office Phone	
Cellular Phone	
E-mail address	
Medical or special care: yes/no	
If yes:	
Comments Text:	

Annex B: Basic Travel Security Rules

(for preparation and during business trips)

For all destinations

Preparation

- Make sure you have valid passport and visa (if needed)
- Scan passport, visa -> erase Social Security Number -> send to own email address, store soft copy in your cell phone
- Ensure you have your AIG insurance card / Policy number and Emergency phone with you
- Ensure your emergency contact data are available and up to date at CILC
- Keep a note of your credit card numbers and the phone number you need to call if you want to block them
- Program important phone numbers into your mobile telephone (including the number of the local Dutch diplomatic mission, home numbers, the emergency number of your travel and health insurers, and local emergency numbers)
- Program the ICE number in your telephone. ICE is the international abbreviation for In Case of Emergency. The ICE number belongs to the person to be called if an emergency occurs. In this case this should be the world-wide 24/7 emergency number: + 31(0)104535656
- Pack your bags so that your hand luggage will contain the most important items:
  - Charged mobile phone + charger (adaptor), including a phone with local sim card (or sufficient roaming capabilities)
  - Valid passport / visa
  - Local currency/credit card. Take cash with you (equivalent of EU500 in a mix of local and international currency). You should not assume that your credit card will be accepted everywhere. For emergencies too it is good to make sure that you can pay a taxi, for example.
  - Medication in original packing, vaccination data and a prescription from the doctor.
  - Number of local contacts and hotel details
- Assure that you are physically and mentally healthy at the moment of traveling.
- Pack to dress conservative/ culturally appropriate.
- Mark your luggage labels only with your business address or the address where you are staying during your trip and your mobile telephone number
- Use suitcase labels that hide your address on the inside
- Don't take valuable items with you if they are not necessary
- Make sure you have enough money in various forms and hide it in different locations
- Keep confidential documents in your hand luggage.
- Ensure you know and understand the Travel Security Policy and related documentation.

During work

- Behave as a guest, do not provoke, avoid cultural/political sensitive discussions
- Should you encounter production strikes, union meetings, and aggression against local management, it is advised to avoid / walk away from the confrontation and think about your own safety.

Hotel Security

- Choose a hotel away from potentially dangerous areas
- Rooms not at ground level, not on the street side
- Avoid rooms too high up, preferably between second and fifth floor
- Be familiar with the hotel lay-out (emergency exits, fire extinguishers etc.)
- At your hotel room:
  - Lock your door and windows
  - Keep your hand luggage and first aid packed
  - Pretend your room is occupied
  - Use spy eye before opening your door

Local transportation

- Check the car on general conditions, safety belts and whether the driver speaks English etc. If you do not trust the car or driver, reject it and call arrange another one.
- Try and position yourself in the backseat, diagonally behind the driver
- Correct the driver when he is speeding or driving dangerous
- Request changes to the car A/C when required (when too cold or too hot)
- Correct the driver when using mobile during driving
- In case of taxi:
  - Agree on the price beforehand
  - Promise a tip if the driver obeys the traffic rules
  - Do not allow other passengers

Leisure time

- The main purpose of your trip is to work. Act accordingly and let leisure under no circumstances effect your ability to meet your work objectives.
- Dress conservative / culturally appropriate.
- Be modest in alcohol consumption. If you want to drink a limited number of alcoholic units, this is best done in the discretion of the hotel.
- If you go out of the city in the weekend, inform the Travel Security Officer of your whereabouts.
- Refrain from dangerous activities.
- Keep your mobile phone switched on at all times.
- Same transport rules apply for leisure time as during working hours.

Addition security rules for medium risk destinations

- Always seek contact with local partners in order to get additional do's and don'ts for this particular destination. Seek advice on means of travelling around and which hotels in which areas to stay (and which to avoid).
- Always arrange a proper pick up from the airport with a pre-agreed meet&greet procedure. Ensure you have the contact details and a charged phone so you can call someone when the meet&greet fails.
- No travelling outside the main cities between sunset and sunrise. Maintain margins for long journeys so that you avoid exposure in case something occurs.
- No self-driving, always arrange a suitable vehicle with driver, preferably via partners. Consult which taxi companies are safe.
- No use of public transport.
- Carry a first aid kit.
- Ensure you know where good hospitals are located in the area that you travel.

Discuss the outcomes of your inquiries/assessment with your Travel Security Officer and agree on a frequency of contact.

CHECKLIST

Subject	Examples	Check
Airport arrival:	Meet and greet procedure by trustworthy entity (ie. in country agent, reputable company, other party)	☐
Transport:	Daily transport, reputable company (eventually need for convoy driving)	☐
	Road safety, speed limits, safety belts, first aid kits.	☐
	Communication during transport necessary?	☐
	Preferred suppliers available?	☐
Accommodation:	Hotel, compound, apartment	☐
	Location of accommodation in relation to the working location (safe route, safe area)	☐
	Fire safety, earthquake safety, in hotels between 2nd and 5th floor.	☐
	Criminal or terrorist activity, security at hotel/accommodation, access control, standoff (distance from public street to hotel entrance).	☐
	Preferred suppliers	☐
Medical:	Availability of medical services. Transport from and to medical services.	☐
	Need for separate medical emergency protocol?	☐
	Additional services from medical service providers needed?	☐
	“What if” scenario’s. Need for first aid kits, defibrillators.	☐
Evacuation:	Likelihood of conflict escalating	☐
	Identification of transport facilities other than commercial flights. Most likely this is done through agreements with the respective governments as a form of consular assistance.	☐
	Identification of destinations to evacuate to	☐
Local cultural and legal issues:	Religious do’s and don’ts	☐
	Alcohol/drugs	☐
	Sexual behavior	☐
Communication:	Satellite phone	☐
	Local simcard	☐
	Frequency of contact	☐

Annex C: Incident Reporting Format

Name of traveler		
Any other persons affected by the incident		
CILC project manager/officer		
Date of Incident		
Nature of the incident		
Description of the incident		
Place of incident		
How was the incident addressed		
Other remarks		
Contact with Emergency Center	When ?	
	Whom ?	
	What ?	
	Follow-up	
Annexes	Please attach copies of any relevant documents: • police report, • witness statements • bills/invoices • claims from third parties • pictures • etc.	

Annex D: Crisis Protocol

Introduction

In case an incident occurs overseas that is of such severity or complexity that line management is unable to manage the case effectively (kidnap/hostage taking of a staff member, non-natural death of a staff member, problematic evacuations etc.) anyone in the organisation can propose the activation of the Crisis Protocol to the Board. The Board will then call this protocol in action and the Crisis Management Team (CMT) will be formed. The Board will decide on the activation (and de-activation) of the CMT. The CMT will then start managing the crisis by insulating the crisis from day-to-day operations.

This Crisis Protocol provides a framework for the necessary steps during a crisis and its immediate aftermath. It is primarily designed for kidnaps and abduction scenarios but it is simple and flexible in order that it might be adapted for a range of other types of security events. The Crisis Protocol withholds the right to arrange its way of working in such a way that is most suitable for the crisis.

The CMT shall remain in place until the crisis and all its consequences are resolved or have been reduced to a severity that can be managed within normal line management.

Composition of the CMT

The CMT consists of the following members (in brackets the foreseen individuals for this position and potential backups):

Crisis Manager:

Central decision maker, responsible for the strategy and overseeing the functioning of CMT.

Crisis Coordinator:

The Crisis Coordinator advises all CMT members on their role and response in relation to this Crisis Protocol and ensures the protocol is followed and decisions are being followed up.

HR Manager:

HR is tasked with coming up with a strategy for family support, staff/volunteer support, post crisis follow-up and deals with insurance and legal issues.

Media manager:

The CMT member tasked with Media is responsible for creating a media strategy which supports the operational strategy of the CMT. He/she implements that strategy, if needed through supporting press officers or spokespersons.

Liaison:

Liaises with external stakeholders such as governments, companies (such as the client) and with the staff present in the country concerned.

CMT Assistant

The assistant to the CMT does the minute taking of CMT meetings, keeps a logbook of all developments (for liability and insurance) and supports the team through logistics. Ensures a visual representation of information and decisions.

Strategy

Directly upon activating the CMT the strategy needs to be defined. Initial strategy is:

- Preservation of life and managing the direct effects of the crisis (in case of a hostage situation this would mean the safe release of the hostages)
- Assure families of victims and agency staff of a responsible and effective response.
- Insulating the crisis from day-to-day operations: ensuring the continuation of the programmes and operations during the crisis and its direct aftermath.
- Fulfil organisational responsibilities and reduce the risk of litigation/liability claims.
- Safeguarding organisational reputation: we want to be and appear competent, authoritative and compassionate.

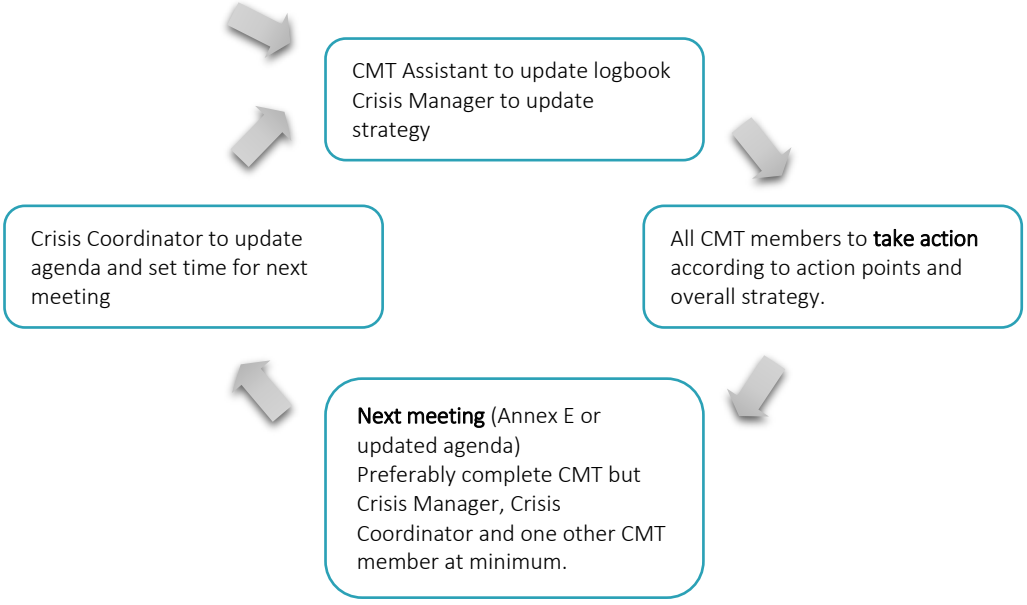
Operation of the CMT

The CMT works with central decision making. This means that all decisions are taken during meetings, and the considerations, decisions and action points are written down by the CMT Assistant. Preferably, all CMT members are present at the meeting and all external communication is scheduled outside the timeframe of the meeting. At least the Crisis Manager, Crisis Coordinator and one other CMT member have to be present to allow decision making.

Report comes in

- MD decides on activation of Crisis Protocol
- CMT is gathered (**Annex A**)
- Company Holding is notified immediately
- Crisis Room is installed (**annex B**)
- CMT Assistant starts logbook (**annex C**)

First Meeting follow agenda (**Annex D**)



Appendix D1 – CMT members and contact details

For every role a replacement is identified and this is the second name for this role. If the primary CMT members is not available or able to come to the Crisis Room within 24 hours, the replacement is contacted.

Role	Name	Primary number	Secondary number
Crisis Manager			
Crisis Coordinator			
HR Manager			
Media			
CMT Assistant			
Liaison			

Other relevant contact details:

IT department:

Directors:

Communications:

Appendix D2 – Crisis Room layout

Upon the activation of a CMT, a room shall immediately be designated as the Crisis Room. Preferably the room is not in a location where its activities generate a lot of attention.

The Crisis Coordinator together with the CMT Assistant will ensure that the room is set up appropriately throughout the crisis.

The room shall be set up with the following equipment/facilities:

- Three landline telephones (with direct lines out, numbers known)
- Two computers connected to the organisation network, internet and Skype
- Speaker phone with recording device and microphone
- Specific email addresses set up for crisis situations to ensure confidentiality (directors assistants, blackberry etc. could cause firewall breach) and to facilitate hand-over to deputy CMT members.
- Easy access to a printer, photocopier and fax machine
- Whiteboard and flip charts (and pens)
- Two clocks (local time and CET time)
- Sufficient chairs and tables for all CMT members
- Maps(s) of country/location concerned
- Basic stationary
- A sign on the door(s) saying “No entry”.
- Television and radio with cable access

Appendix D3 – Logbook

Logbook *example*. To be projected on the wall and updated as a minimum after every meeting. CMT Assistant is responsible for maintaining the logbook.

Time	What (event)	Decision	Action by	Received	Done
1st meeting, 1400hrs	3x staff missing	Activate CMT, inform BoD	DD	BoD	x
		Inform specialist company, request assistance	Crisis Coordinator		x
		Media statement, reactive line 1	Media	Media support	x
		Inform all staff regarding incident	HR	Staff support	
2nd meeting 1430hrs					

Appendix D4 – Agenda first meeting

1. Reason for the establishment of the CMT – Crisis Manager

- Presentation of available facts
- Identification of information gaps
- Actions taken so far

2. Crisis Protocol – Crisis Coordinator

- Overview of CMT approach and/or related procedures (central decision making through agenda, meetings, action points)
- Confirmation of individual CMT member roles
- Confirm key contact in country of operations
- Is contact in country capable of responding? Need for support (staff, logistics, guidance)
- Do we foresee the need for external assistance?

3. Crisis resolution – Crisis Manager

- Are there any immediate steps that should be taken?

4. Human Resources

- Can and should we notify staff, in the Netherlands or elsewhere?
- Do we need to inform reception (for incoming calls or visitors?)
- Can and should we notify family of the victim(s) at this stage?

5. General Crisis Management – Crisis Manager

- Confirm contact details and ongoing availability of all CMT members / deputies
- Confirm time/date of next meeting

6. Summary of key decisions / action points – Crisis Coordinator

- Confirmation of all action points agreed at meeting

Appendix D5 – Agenda second meeting

1. Crisis Coordinator

- Review action points from previous meeting
- Brief update on available facts

2. Liaison

- Update on field situation
- Do we need to contact the relevant governments/embassies?
- How is the key contact in country doing? Are they in need of any support?
- Are we prepared for (the next) contact with hostage takers? Who is likely to receive this call and are they instructed? Guidance in Appendix F

3. Human Resources

- What support is required for remaining Company staff? Should they have (more) information on the situation? Is reception informed?
- Do we have a full picture of the victim(s) family and/or partner(s)?
- Do they feel supported by Company?
- Do we have contact with insurer(s)?
- Reception plan? Psycho traumatic support for staff, victim(s), family?

4. Media

- Review of communication about this crisis in the public domain?
- How are we managing the media?
- COMPANY's communications plan

5. Crisis Manager

- What are the next steps? Are our actions still in line with our strategy and do we need to update this?
- Does the CMT has the capacity, resources and resilience to manage this crisis effectively?
- Confirm time/date of next meeting

6. Summary of key decisions / action points – Crisis Coordinator

- Confirmation of all action points agreed at meeting
- Is this agenda fit for purpose? Changes?

Appendix D6 – Guidelines for the untrained negotiator

HOW YOU RESPOND TO THE KIDNAPPER(S) WILL SET THE TONE OF THE INCIDENT.

PREVENT IT GETTING WORSE BY BEING PREPARED TO NEGOTIATE.

DO NOT ignore communication from the kidnapper(s). Frustration may be dangerous. This is not a power struggle you will win by challenging words or psychology. SO SPEAK TO THEM!

ALWAYS be ready to receive messages.

DO ASK: Who are you, what would you like to be called?

Remember the name! – Give yours

What is this all about? What has happened?

PERSONALISE the hostages; refer to them by their first name.

Do say; ‘don't harm anyone’. Try to speak to them to obtain 'Proof of Life' and give reassurance

BUT Try to avoid use of words
'Kidnap, hostage, demand, deadline, ransom, proof of life, surrender',

DO keep a record of what you do, ideally by tape, if not available make a written note ASAP.

ACTIVE LISTENING: Listen to the content and more importantly how they say it as an indicator of the real emotions being expressed

DO NOT challenge a kidnapper to carry out threats but point out that such action will not help anyone, continue to seek proof of life.

DO NOT ask for DEMANDS, there may not be any!

DO NOT represent yourself as the final decision maker, i.e. 'the person in charge'

DO NOT make promises. Say, "I will see what I can do".

DO NOT set yourself DEADLINES. Never say, "I will do that in ten minutes" but introduce doubt, "I will try to get that done as quickly as possible".

DO NOT ask for DEADLINES
Never say, "How long have I got to do that".

DO NOT accept the kidnapper(s) DEADLINES without comment but introduce doubt. "I hear you but it will be very difficult to do what you want in the time you say".

DO NOT assume you can have a private conversation with a hostage, particularly to gather information. The kidnapper(s) may be listening.

DO NOT negotiate if you are the Crisis Manager.
You CANNOT do both jobs competently.