Concern's Security Policy

March 2016

Contents

Introduction
Founded in response to the famine in Biafra, Concern is a global organisation with offices in Ireland, the UK, the US and the Republic of Korea, supporting operations in the world's poorest and most vulnerable contexts.

Our Identity
Concern is a non-governmental, international, humanitarian organisation dedicated to the reduction of suffering and working towards the ultimate elimination of extreme poverty in the world's poorest countries.

Our Vision
Is a world where no-one lives in poverty, fear or oppression; where all have access to a decent standard of living and the opportunities and choices essential to a long, healthy and creative life; a world where everyone is treated with dignity and respect.

Our Mission
Is to help people living in extreme poverty achieve major improvements in their lives, which last and spread without ongoing support from Concern. To achieve this mission we engage in long term development work, build resilience, respond to emergencies and seek to address the root causes of poverty through our development education and advocacy work.

Our commitment to security
While the security of all Concern staff is of paramount importance, it cannot be completely guaranteed in every situation. Concern recognises that the nature of our work places great demands on staff, especially those working in high risk contexts, where conflict, criminality and other forms of violence that may cause acute anxiety, put them in harm's way, and/or pose a threat to their lives.

Consistent with the duty of care that we have to all of our staff, Concern is committed to developing procedures and practices aimed at putting appropriate security measures in place to allow staff to establish and maintain presence and continue to deliver programmes in some of the most insecure places in the world. The following principles have been developed to support this duty.

While recognising that maintaining a presence in our programme areas is our preferred way of working, there may be times when the remote management of programmes is required to address acute humanitarian needs and fulfil our mandate.

Purpose and scope of this policy
This document sets out the policy for the security of staff, official visitors, and the dependants of international staff who have accompanied status, by defining basic security principles applicable to all Concern staff and programmes.

Concern's definition of security is that it seeks to address threats derived from human action. Health and safety issues, including accidental hazards such as car accidents, fires or medical emergencies, are not covered here.

All staff must comply with this policy.

Failure to comply with this policy, and the security management procedures outlined in the Security Management Plans (SMPs) of our countries of operation, may increase the risk of harm to staff, assets, and other development and humanitarian workers. It may also reduce acceptance of Concern by host governments, communities, and beneficiaries. Any non-compliance, including failure to report breaches of this policy, may result in disciplinary action up to and including dismissal.

Principles

1. Priority to human life

The security of personnel is of the highest priority for the organisation, ranking ahead of the protection of assets, including premises, vehicles, office equipment or programme materials.

Given the profile of countries in which Concern works, good judgement is required with regard to continued programming and presence.

It may be necessary for staff to operate in contexts of considerable insecurity if this allows life-saving programmes to be delivered. In such circumstances, our security management practice must be adapted to this heightened level of risk.

Our security practice must remain adaptive to and commensurate with the threat level that exists in all of our areas of operation.

2. Staff have responsibilities and rights

Security is an on-going, collective responsibility, and each member of staff is obliged to:

- ensure that they receive an adequate security briefing and are aware of security risks in their area and country of deployment, and of their responsibilities in relation to personal and team security
- actively participate in and contribute to the maintenance of good in-country security practice (especially the country programme SMP)
- be responsible for their own security and the security of staff they manage
- be responsible for Concern assets under their management
- where possible, support the security practice of implementing partners and beneficiaries, including programme design and delivery
- behave as a positive representative of Concern, ensuring appropriate behaviour and adherence to the *Programme Participant Protection Policy* (the P4) and the *Concern Code of Conduct*

International staff with accompanied status are required to ensure that their dependents are aware of and comply with the security procedures which apply in their country of deployment.

All staff are responsible for reporting to their line manager any action or behaviour that breaches this policy or the country programme SMP that may jeopardise individual or team security and/or Concern's reputation.

Such reports will result in a confidential and prompt investigation. Staff reporting possible violations and/or involved in such investigations will be protected against any form of intimidation, threats, reprisal or retaliation resulting from the alleged incident. Any member of staff found to be intimidating or retaliating against a person making a complaint or assisting in an investigation will be subject to disciplinary action.

As an organisation, Concern commits to ensuring that:

- SMPs are developed and maintained in all countries of operation
- all staff will receive security briefings relative to their country or area of operation
- countries targeted for specific security training will adequately engage with the training process
- periodic security reviews or audits will be conducted of higher risk countries, or of countries in which there has been a significant security incident
- staff understand the security contexts and risks in their places of work and their duty to adhere to the security management procedures that have been put in in place to address these

3. Security management responsibility

The Chief Executive Officer (CEO) is responsible to Concern's Council for the security of all staff.

Operational responsibility for security management follows the line management structure. In Dublin, the International Programmes Director and the Emergency Director are responsible to the CEO for the security of all staff working for Concern overseas. The day to day management of security procedures may be delegated to the Regional Directors.

At a country programme level, responsibility for staff security rests with the Country Director. The day to day management of security may be delegated to a Security Focal Point.

Those responsible for managing staff security must ensure that:

- security management tasks are delegated and implemented by staff with sufficient competence and time to deal with the relevant issues
- an SMP and appropriate practice are developed, implemented and maintained in a manner consistent with Concern's *Approach to Security Management, Planning and Practice* (SMP2)[1]
- Security Focal Points and the establishment of Security Focal Groups are appointed in each location
- all staff and visitors are updated on security incidents or issues and related management decisions in a timely manner
- an adequate communications system is in place
- all staff and visitors are briefed on the security situation and practice that are in place in their locations in a timely manner
- all staff and visitors adhere to these
- adequate time and resources are given to security management, including co-ordination

Concern will never delegate security management to others, whether NGOs, UN agencies, security co-ordination platforms, or military forces, etc. All country programmes must develop and maintain their own security management practice, the capacity to undertake security risk analysis, and the ability to adapt their practice to changes in their operating context.

4. Organisation policy responsibility

The Emergency Director is responsible for developing the Security Policy, monitoring its implementation, and for advising the Senior Management Team and Council on security matters. Permission to adopt practices that differ from the policy can only be granted by the CEO.

5. Staff skills and capacity

Concern will endeavour to ensure that all key staff, especially managers and members of Security Focal Groups have the necessary skills and capacity to analyse potential security threats in their working environment and to put in place appropriate measures to reduce their vulnerability to these. This will be achieved through appropriate recruitment, training, the active dissemination of country specific SMPs and on-going good communication and security management practice.

6. No operations without SMPs

A country specific SMP must be developed and maintained in a timely manner for every country in which Concern works.

In countries with regional or field offices for which there are different security risks, location specific contextual analysis and standard operating procedures (SOPs) are also required. All SMPs must follow the *Approach to Security Management, Planning and Practice* and the template appended to it.

Prior to the establishment of any significant new programme intervention or area of operation, a location-specific context and risk analysis must be undertaken.

[1] SMP2 and the accompanying template for the development of SMPs can be found on the Emergency Directorate's intranet page: Reference and Support Documents > Security Management folder > SMP2 Security Management Planning and Practice - EMU April 2012 folder

It is the responsibility of the Country Director to review the SMP before it is submitted to Dublin for approval. In Dublin, the Emergency Directorate will review it for consistency with the *Approach to Security Management, Planning and Practice* and for the appropriateness of the SOPs, and provide feedback to the relevant Regional Director as to whether the draft SMP is of an acceptable standard. The Regional Director must provide feedback to the Country Director and, if it is of an acceptable standard, approve the SMP. If it is not, a further version must be produced by the country programme in a timely manner.

Each SMP must be regularly updated in accordance with the agreed frequency for review.

All staff must be made aware of the contents, application, intent and binding nature of the SMP.

In countries in which Concern does not have a presence, but to which we want to send staff to conduct an assessment or to attend a workshop, etc., a rapid security review must be conducted through contact with other organisations already present on the ground. Any such review should include consideration of the proposed venue for workshops, training, etc. Approval for such deployments can only be made by the Country Director for country programme staff, and by the relevant line manager for Dublin-based staff. There must be clarity in relation to insurance, security and evacuation protocols in all such instances.

7. Programme design and standards

The central element of our approach to security management is through building and sustaining acceptance for our presence and programmes from the communities within which we work, their governments and, very often, armed groups holding a degree of control or authority in our areas of operation. It is essential that we engage all relevant stakeholders in the identification and design of our interventions and consider the impact of these on local power dynamics and the potential vulnerability for the target populations arising from our interventions. Programme choice, design, quality, scale and the mechanism for delivery all affect the degree of acceptance that might be gained from the community and those in positions of influence and power in our areas of operation. As such, all countries of operation are required to adhere to the *Code of Conduct*[2], the Sphere Project's Humanitarian Charter and Minimum Standards, the accountability requirements of the Core Humanitarian Standard, the P4 and Concern Code of Conduct, staff recruitment procedures and other relevant organisational policies and guidelines.

8. Right to Withdraw

Staff may withdraw from a programme area if the security situation deteriorates rapidly and relocation is a more prudent option than hibernation. Ideally, this decision should be taken in consultation with their line manager, but if the circumstances mean that this is not possible, then staff have the right to withdraw from an area without the approval of their line manager.

In the event of any such withdrawal, a full review of the decision will be undertaken by the country management team. In exceptional circumstances, or if there is a clear disagreement between the staff member and his/her line manager in relation to the level of insecurity in an area, this review may be carried out by someone from outside of the country programme.

9. Decision to deploy

Irrespective of the judgement of the organisation, any staff member may decline to take up work in, or travel to, an area if s/he feels uncomfortable with the frequency or level of risk in that area. In the event of such a situation, a review will be undertaken between the individual and his/her line manager to determine an appropriate course of action in relation to future deployment/employment. For country programme based staff, the relevant Regional Director must be advised of the process and the outcome. For head office staff, this review should be conducted with the staff member's line manager and the outcome reported to the relevant Director.

[2] *The Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief.*

10. All security incidents must be reported

All staff have a duty to report all security incidents to the Country Director who must, in turn, report them to the respective Regional Director in a timely manner. The International Programmes Director and the Emergency Director must be copied on all security incident reports to enable tracking, monitoring and analysis of security trends.

Guidance as to what constitutes a security incident is presented in the *Approach to Security Management, Planning and Practice*.

As soon after the incident as possible, a post-incident report must be completed by all of those involved in or affected by the incident, to allow for an analysis to be undertaken so that the Country Director may determine why the incident happened, whether it could be prevented, and how such incidents may be managed more effectively in the future. In the event of a particularly serious incident – such as the decision to withdraw from a programme area – an external review may be conducted.

The family members of staff involved in security incidents should not be contacted by Concern unless this has been approved by the Country Director in relation to national staff, or by the International Programmes Director or Emergency Director for international staff.

11. Kidnap/Abduction

Concern's policy is not to pay ransoms for the release of staff.

In the event that a member of staff is abducted, contact should be made as soon as possible with the Dublin office so that action can be co-ordinated between the Crisis Management Team the country programme's Incident Management Team. Reporting of incidents should generally follow the line management structure - i.e. by the Country Director to the Regional Director, but speed is of the essence in these cases and incidents should be reported directly to relevant members of the Dublin Senior Management Team (SMT) as quickly as possible.

The CEO will assume ultimate decision making responsibility and decide whether to convene an organisational Crisis Management Team (CMT). At the country programme level, the Country Director should establish an Incident Management Team (IMT).

Concern will provide appropriate support to immediate family members during the period of the kidnap. The CMT will manage media relations and liaison with family members.

Full details on the management of the CMT and IMT can be found in the *Crisis Management Plan*, February 2016.

12. The use of armed protection is discouraged

Concern staff should seek to avoid using armed protection, as it may be perceived to compromise our neutrality.

This is not an absolute - in circumstances of instability, or where it is a requirement of the government or local authorities for vehicles to be escorted by police or military personnel - armed protection can be considered.

Concern does not rule out the employment of armed guards for the protection of equipment and facilities, including refugee or IDP camps, particularly in areas where violent crime is common. However, the nature of this protection must be considered in light of the local context and the possible impact that its utilisation may have on the local perception of Concern.

Permission to use or hire armed guards (either directly as Concern staff or indirectly through the hiring of staff via a security company) may only be given by the respective Regional Director in consultation with the International Programmes Director or the Emergency Director.

Firearms should not be carried in Concern vehicles unless the security situation demands this, and may only occur if the Country Director has approved this following consultation with the relevant Regional Director.

Other than those people specifically employed to provide armed protection, Concern staff must not carry arms while on Concern duty.

Armed escorts may only be used in exceptional circumstances and with the approval of the Regional Director in consultation with the International Programme Director or Emergency Director[3]. Any such approval is not open-ended. It is limited to a period of six months and cannot be extended beyond this without further review and approval.

13. Limit involvement with armed forces to essential humanitarian actions

In determining the relationship between Concern and military forces, we should be guided by the *Code of Conduct*[4]. Engagement with military forces is a difficult area to be entirely prescriptive on, with local circumstances informing this, but humanitarian agencies must maintain their independence of decision-making and action, and can never operate under the command of the military.

In those situations in which international peace keeping forces have been deployed to a country, there may be a need to share certain types of information, particularly with regard to security, conditions in shared space (transport, aid movements, common use airfields), general estimates about the scale of the emergency, etc. In some conflict contexts, especially those in which there is aerial bombardment, deconfliction processes may require the sharing of GPS co-ordinates of offices, warehouses, residences, etc. with military forces.[5]

However, information should not be shared if it could in any way endanger communities or risk staff security, and must be guided by the *Code of Conduct* principle that we never act as instruments of the foreign policy of donor governments.

14. Plan and prepare for evacuation or relocation based on contractual relationship

Planning and preparation for evacuation and relocation are integral parts of security management, and SOPs for these measures must be included in all SMPs. Preparation should also be made for hibernation.

Concern has different obligations for national and international staff because of the different contractual relationships that we have with them. Our obligations to national staff are informed by national labour laws. Country-level SMPs must reflect these laws, and it is the responsibility of each country programme management team to ensure that national staff contracts and the SMP are fully compliant and consistent.

Concern has a contractual responsibility to return international staff (and their dependants if they have accompanied status) to their country of residence, and to evacuate or relocate them from their place of work should it become necessary.

Concern is not obliged to relocate locally employed national staff within their home area.

---

[3] For reference, see *IASC Non-Binding Guidelines on the Use of Armed Escorts for Humanitarian Convoys* and the Concern guidance note on the use of armed escorts.

[4] Article four of the Code of Conduct states: *We will never knowingly - or through negligence - allow ourselves, or our employees, to be used to gather information of a political, military or economically sensitive nature for governments or other bodies that may serve purposes other than those which are strictly humanitarian, nor will we act as instruments of foreign policy of donor governments.*

[5] In most instances, deconfliction processes are co-ordinated through OCHA.

However, Concern has a responsibility to relocate national staff who have been seconded to work in an area of the country other than their home area, or who are temporarily visiting a programme area.

While having no contractual obligation to do so, Concern may, in exceptional circumstances, seek to relocate staff who may be particularly vulnerable to attack.

It is the responsibility of the Country Director to ensure that Concern's responsibilities to all staff and the dependants of international staff with accompanied status are made clear at the time of appointment, and are clarified and communicated on a regular basis, or as circumstances change.

The SOPs for evacuation, relocation and hibernation must also include details of arrangements for national staff to assume responsibility for offices and programmes in the event of the evacuation of international staff. These arrangements can only be put in place if they do not place staff at an unacceptable level of risk and must be agreed in advance with the relevant staff to ensure that they are willing and able to take on such roles, and arrangements for this must be in place.

15. The order to withdraw

15.1 From a programme area

The order to withdraw from an area can be given by the local manager with immediate effect and is binding on all staff and visitors. Where possible, the local manager should consult the Country Director or his/her line manager before ordering a withdrawal, but if this is not possible, then s/he should make the decision to withdraw.

The Country Director may direct a team to withdraw from a project area, may suspend or close an office/programme, and may override a local manager's wish to remain in the programme area. However, a Country Director may not override a local manager's decision to leave an area if the local manager deems the situation to be too insecure to remain.

The decision to suspend or temporarily close a programme must be approved by the Country Director in consultation with the Regional Director.

15.2 From a country

The decision to evacuate individual international staff from a country should be taken by the Country Director in consultation with the Regional Director.

The decision to evacuate all international staff or to suspend activities in a country, must only be taken by the International Programmes Director or the Emergency Director in consultation with the Chief Executive Officer.

16. The decision to stay

If, following a serious security incident targeting either Concern or other organisations working in our programme area, a decision is taken for the team to remain and continue delivering programmes in the area, the Country Director is required to provide a justification for this decision which must be approved by the Regional Director and the International Programmes Director or the Emergency Director as appropriate.

17. Authorisation to return

17.1 To a programme area

Authorisation to return to an area after evacuation, relocation or programme suspension can only be taken after a systematic security review has been undertaken and a written report with clear recommendations has

been submitted to the Regional Director and the International Programmes Director or the Emergency Director for approval.[6]

17.2 To a country

Ultimately, the decision to return to a country following an evacuation may only be taken by the CEO and must be preceded by the completion of a full security review.

18. Security co-ordination and information sharing

Concern will coordinate closely with other humanitarian agencies in managing its security, including with the UN through the Saving Lives Together process. Security incidents should be reported to other agencies and to security co-ordination mechanisms if these exist in our countries of operation.

Security Focal Points must be appointed and Security Focal Groups (SFGs), established in all locations to liaise, coordinate and advise managers on security related issues. The SFGs should ensure that all staff contribute to security management and are informed of all security incidents and practices that relate to them.

19. Universal application of principles

The security principles outlined above apply to all Concern country programmes without exception. All countries must develop their own SMPs and adhere to the Security Policy.

20. Review and reporting process

20.1 The policy

In recognition of the fact that both internal and external environments change, the scope and content of this policy will be reviewed periodically. This review process will, in line with Concern's values, be consultative and participatory in nature.

The responsibility for initiating the process rests with the Emergency Director on the Concern Dublin SMT and with Council.

20.2 The operating environment

On an annual basis, the Emergency Director will provide a report to SMT and Council outlining:

- any changes in the global security environment
- any serious security incidents that have been reported in the previous year and how they have been addressed
- key issues arising in the security audits and reviews carried out during the course of the year
- updates on security training carried out in the previous year
- security-related plans for the coming year

[6] All such security reviews should be consistent with the *Approach to Security Management, Planning and Practice*.

Glossary of terms used in this policy

Acceptable Risk
The 'threshold of acceptable risk' is the point beyond which the risk to the lives or safety of staff delivering programmes or remaining in a programme area is considered by the organisation to be too high. The threshold is determined by the probability that an incident will occur and the seriousness of its impact on the organisation if it does so. Concern does not expect any staff member to be killed, kidnapped or seriously injured as a consequence of working for the organisation and will take all reasonable measures to ensure that this does not happen.

- **Acceptable risk** is when we are confident that our risk analysis and the measures that we have put in place to manage identified threats are sufficiently robust to reduce the likelihood of events happening or, if they happen, to reduce their impact upon us to a level that does not have unacceptable consequences.

- **Unacceptable risk** is when, despite our analysis and the measures we have put in place to reduce the risks that exist, we feel that the level of threat to our staff is at a level that is not warranted by the nature of programmes that we are delivering.

Actors
Individuals or members of informal or formal groups who may, directly or indirectly, pose a threat to us by their actions.

Deconfliction
In the humanitarian context, is the sharing of information and planning advisories between humanitarian agencies and military actors to prevent or resolve conflicts between the two, remove obstacles to humanitarian action, and avoid potential hazards for humanitarian workers. It may include the negotiation of military pauses, temporary cessation of hostilities or ceasefires, or safe corridors for aid delivery, or sharing the details of the physical location of staff and assets with combatants to reduce the potential for accidental or collateral bombardment.

Duty of Care
Duty of care refers to the moral and legal obligations that employers have to their workforce to maintain their wellbeing, security and safety and to take practical steps to mitigate foreseeable dangers. It includes the duty to disclose the risks inherent in a programme area and any material or specific risks associated with Concern's operations in that area.

Evacuation refers to the repositioning of staff across international borders (see also hibernation and relocation).

Hibernation refers to staff having to go into lock-down - usually at the Concern office, residences, or another pre-arranged place (see also evacuation and relocation).

Informed Consent
Informed consent requires employers to ensure that their staff understand the security contexts and risks in their places of work and their duty to adhere to the security management procedures that have been put in place by their organisation to address these.

Relocation is the withdrawal of staff from one part of the country to another (see also evacuation and hibernation).

Security Focal Group (SFG)
Members of staff should be chosen to reflect the staff profile in each location in terms of programmes, ethnicity, national and international status, job function and gender. An SFG should ensure wide participation of and consultation with all staff, collecting security-related information from and sharing information and analysis with them, and bring a good understanding of the local context through their social, family and professional contacts.

Security Focal Point (SFP)
SFPs are the designated principal conduits for channelling security information within the country programme, including between local and national SFPs and their respective SFGs. SFPs must remind managers and staff of their obligation and responsibility in ensuring that agreed security measures are followed. An SFP must be identified for each location in which we have an office.

Security Measures
There are three broad set of measures we employ in trying to manage security risk:

- **Acceptance** is the pro-active gaining and maintaining of support for our presence and programmes by programme participants, the larger community in which we work, and local power-brokers.
- **Protection** describes physical and procedural measures that focus on reducing our vulnerability.
- **Deterrence** measures are ones that seek to prevent a potential incident from occurring by posing a counter-threat.

Security Threat
A security threat is a potential danger posed by an actor that puts our staff in harm's way or in a state of acute anxiety. It may also result in the loss of or damage to our assets. Either of these consequences can compromise our capacity to deliver effective programmes. Collectively, the threats identified amount to the **security risk** in a given area.

Security Threat Analysis
A systematic scrutiny of the potential threats in a given area in terms of who poses them, where and when they are most likely to occur, and trends in these. This analysis will inform our choice of security measures.

Vulnerability
Our vulnerability as an organisation is determined by the degree to which our staff and assets are exposed to threats, the nature of those threats, and any factors or actions that potentially increase or decrease the impact of a security incident.

A caution
It should be noted that the contextual analysis in country-specific SMPs may contain information or opinions that we may not want to be shared with all staff or to be in the public domain. The Country Director will be expected to use his/her judgement in deciding which parts of the SMP are made available to which staff and the extent to which it may be shared with other organisations.