Oxfam Security Policy

APPROVED BY MEDs 11 03 2014

Table of Contents

Introduction 3
Purpose 3
Complementarity with other Governing Frameworks & Codes 3
Applicability and Policy Implementation 4
Security Management Approaches 4
Risk Attitude & Risk Tolerance 5
Principles 7
Duty of Care & Security of Personnel 7
Risk Ownership & Delegation 7
Informed Consent & Right to Withdraw 7
Individual Obligations & Self Generated Risks 8
Gender and Security 8
Non-Discrimination & Equality of Risk Treatment 8
Data Protection & Digital Security 8
Responsibilities 9
Individual Employees 9
Line Managers - Generic 9
Line Managers - Country Directors & Associate Country Directors 9
Other Directors & Executive Officers 9
Security Working Group (SWG) 10
Governing Bodies (e.g. Boards, Councils, etc.) 10
Security Levels 10
Security Management Plans 10
Security Incident Reporting 10
Evacuation, Relocation & Hibernation 11
Implementing Partners 11
Use of Armed Protection 11
Engaging with Armed Actors 11
Crisis Management 12
No Ransom or Other Concession 12
Training, Learning & Development 12
Annex A: Oxfam Code of Conduct 13
Annex B: Oxfam Security Protocol 16
Annex C: Security Levels 19
Annex D: Security Management Plan Template 20
Annex E: Crisis Management Plan Template 21

[format note – page break]

Introduction

Oxfam is an international confederation of 17 organizations networked together in more than 90 countries, as part of a global movement for change, to build a future free from the injustice of poverty.[1] To achieve this goal Oxfam uses a combination of rights-based sustainable development programs, public education, Fair Trade, campaigns, advocacy, and humanitarian assistance in disasters and conflicts.[2]

The Oxfam confederation is made up of non-governmental organizations that employ thousands of people around the world. Many of these people live and work in hazardous and insecure environments. As responsible employers, Oxfam members acknowledge their obligations to provide, safe and secure workplaces, where fair, just and reasonably practical for employees. In appropriate circumstances, and depending on the nature of the relationship, there may also be obligations to associated personnel.[3] Meeting these obligations requires Oxfam to manage risks, without being risk-averse.

This text uses terms and definitions from the international standard ISO 31000:2009 Risk Management – Principles and Guidelines as well as sector-specific good practices. Definitions are footnoted throughout. Unless indicated otherwise the term "Oxfam" refers to the collective membership of the Oxfam confederation, and is an abbreviated version for "Oxfam Affiliates" and "Oxfam International".

Purpose

The purpose of the security policy is to record and communicate the guiding principles and responsibilities that form the governing framework for security risk management.

The policy provides managers and staff direction and guidance to enable Oxfam's programme objectives to be effectively implemented while at the same time protecting (to the extent possible) Oxfam's employees, reputation and assets from harm.

Complementarity with other Governing Frameworks & Codes

Several governing frameworks guide Oxfam's program and operations management and shape Oxfam's overall behaviour and approach to its work. The security policy forms part of the set of governing codes and agreements that Oxfam willingly commits to.

The security policy is complementary to the following governing frameworks:

- Oxfam Code of Conduct[4]
- Oxfam Security Protocol[5]
- Oxfam Single Management Structure Agreement (SMA)[6]
- People in Aid Code of Good Practice[7]

[1] Oxfam mission statement, http://www.oxfam.org/en/about
[2] Oxfam purpose and beliefs, paragraph 3, http://www.oxfam.org/en/about/what/purpose-and-beliefs
[3] **Associated personnel** are persons who are not employees but who are engaged by Oxfam for the purpose of supporting or delivering the organization's programs. Associated personnel may include volunteers, interns, consultants, or official visitors.
[4] Refer to Annex A – Oxfam Code of Conduct, https://sumus.oxfam.org/oi-secretariat/documents/code-conduct-policies
[5] Refer to Annex B – Oxfam Security Protocol, https://sumus.oxfam.org/security-administrators/documents/oxfam-security-protocol-2013
[6] https://sumus.oxfam.org/single-management-structure-group/documents/sma-final-july-2011
[7] http://www.peopleinaid.org/pool/files/code/code-en.pdf

- The Code of Conduct for The International Red Cross and Red Crescent Movement and NGOs in Disaster Relief[8]
- OI and Security Crisis Management: Recommendations of the OI Security Network Working Group[9]
- Guidance Note: Obtaining Authorisation to Use Armed Escorts/Guards: An Exception to the OI Security Protocol[10]
- SCHR Position Paper on Humanitarian Military Relations[11]

Where necessary the governing frameworks are referenced in the policy. However the complementarity noted above is not intended as a cross-referencing guide to readers. Complementarity refers to the **security policy forming part of a specific set of governing references**, and as such communicates policy positions and principles that are aligned with, supportive of, or analogous with the other codes and agreements.

Applicability and Policy Implementation

The security policy applies to Oxfam organisations (as independent legal entities and employers), and their employees. In certain circumstances, and depending on the nature of the relationship, the policy may apply to associated personnel. The security policy shall be routinely implemented as part of program or operational management activities.

The Oxfam Security Protocol[12] outlines the architecture by which security will be managed. It is acknowledged that the local operating context will influence how the security policy is put into practice, however the principles contained in the policy shall be reflected in local security and/or crisis management plans and procedures.

Security Management Approaches

Security must be actively managed, not just planned for, and is most effective when fully integrated into program management. Managers must ensure security of persons and programs is given a high priority, through objective setting, the performance management cycle, work planning/scheduling and other relevant management tools. Security management approaches are informed by an understanding of the local context and based upon the outcomes risk assessments. Generally approaches are not mutually exclusive; the key is to adopt the right mix in a given context.

Acceptance approaches reduce or remove threats by gaining widespread acceptance (political and social consent) in the community for Oxfam's presence and activities. Building positive relationships and promoting understanding of Oxfam through establishing our legitimacy as an impartial and independent[13] humanitarian actor, achieves this. This identity must be communicated clearly to all parties. The success of an 'Acceptance' approach depends on many factors including staff behaviour, staff diversity, type, design and implementation of programs, community participation, choice of partners and proactive creation and maintenance of relationships.

[8] http://www.ifrc.org/en/publications-and-reports/code-of-conduct/
[9] https://sumus.oxfam.org/security-administrators/documents/recommendations-crisis-management-protocol
[10] https://sumus.oxfam.org/oxfam-gb-aim-3-meeting-jan-2012/documents/guidance-note-obtaining-authorisation-use-armed
[11] https://docs.unocha.org/sites/dms/Documents/Steering%20Committee%20for%20Humanitarian%20Response-%20SCHR%20position%20paper%20on%20humanitarian-military%20relations%20(2010).pdf
[12] Refer to Annex B – Oxfam Security Protocol: https://sumus.oxfam.org/security-administrators/documents/oxfam-security-protocol-2013
[13] Oxfam is a signatory of, and holds itself accountable to, the Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief

Protection approaches aim to reduce risk by reducing vulnerability, through protective devices and operating procedures. Protective devices can be communications equipment, reliable vehicles, use or non-use of Oxfam's branding (e.g. displaying the logo), or perimeter protection for premises. Operating policies and procedures include locally based security management plans and standard operating procedures (SOPs), including evacuation plans, equitable staff policies, and other program management policies and procedures relevant to the local context.

Deterrence approaches aim to reduce risk by containing or deterring the threat by applying a credible counter-threat (e.g. suspension or withdrawal of activities, or the use of armed guards *in exceptional and authorised circumstances only*, or calling for military intervention. This approach is generally to be considered as a last resort, and is decided according to specific procedures and authorisation levels.

Risk Attitude & Risk Tolerance

Almost every operational activity presents threats to personnel and assets. Guided by the humanitarian imperative,[14] Oxfam's risk attitude[15] is aligned with its mission statement. Oxfam will **always assess and communicate the level of risk** in a given context and take informed management decisions to accept or avoid these risks.

The humanitarian imperative is reiterated in the security policy as a reminder to employees that acting in a safe and secure manner enables Oxfam to meaningfully uphold the rights of this fundamental principle.

> *"The right to receive humanitarian assistance, and to offer it, is a fundamental humanitarian principle which should be enjoyed by all citizens of all countries. As members of the international community, we recognise our obligation to provide humanitarian assistance wherever it is needed. Hence the need for unimpeded access to affected populations is of fundamental importance in exercising that responsibility. The prime motivation of our response to disaster is to alleviate human suffering amongst those least able to withstand the stress caused by disaster. When we give humanitarian aid it is not a partisan or political act and should not be viewed as such."*[16]

Risk assessments aim to provide information in sufficient detail in order for managers and other employees to take informed decisions. Oxfam's risk assessments shall take account of the following minimum considerations:

- The specific operating context and regional influences
- The foreseeable threats to personnel and programs
- The impact foreseeable threats may have on Oxfam's personnel and programs
- The factors that expose or make Oxfam vulnerable to these threats
- The available options to treat the risks presented by these threats

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

[15] **Risk attitude** is defined as **t**he organization's approach to assess and eventually pursue, retain, take or turn away from risk; (ISO 31000/2009 & ISO Guide 73/2009)

[16] http://www.icrc.org/eng/assets/files/publications/icrc-002-1067.pdf

Oxfam's tolerance[17] to take risks will **always take account of program objectives and the importance of what is to be achieved,** as well as the impact of other strategic factors (e.g. impact of key relationships, donor interests, etc). Risk owners[18] will decide on a case-by-case basis whether the specific program objectives and intended outcomes justify accepting the assessed level of risk. It is important to note that Oxfam works in some of the most challenging, hazardous and dangerous environments. When humanitarian needs are high, Oxfam may accept a higher level of risk. In such situations an even greater emphasis on security management is essential.

[format note – page break]

[17] **Risk tolerance** is defined as the organization's readiness to bear [accept] the risk in order to achieve objectives; (adapted from ISO 31000/2009 & ISO Guide 73/2009)

[18] **Risk owners** are the persons with the decision making authority and accountability to manage risks; (ISO 31000/2009 & ISO Guide 73/2009)

Principles

In the context of the Oxfam security policy, **principles** contain the overarching rules and beliefs that govern Oxfam's approach to security management. The principles are intended to provide clarity to certain policy positions and guide risk management decisions and actions.

Duty of Care & Security of Personnel

Security of personnel (whether employees or others) shall always remain a higher priority than the protection of material assets, the preservation of programs, the expression of advocacy objectives, or the protection of Oxfam's reputation.

Oxfam's duty of care is exercised through the application of the security policy, and other management policies and procedures. The systems developed to manage duty of care include (but are not limited to) informing employees about work-related risks, preparing employees to manage and treat risks, and seeking to ensure post-incident care (e.g. counselling for victims, their families, and/or colleagues) is available to employees.

Risk Ownership & Delegation

Security management is a line management responsibility in Oxfam. All Oxfam employees and the various governing boards and executive officers are risk owners. Risks owners are defined as *"the persons with the decision making authority and accountability to manage risks."*[19]

The exact level of risk ownership, accountability and responsibility of these individuals or collective bodies will vary depending on their assigned roles, and may be influenced by national laws or regulations concerning legal liabilities.

Risk ownership and the subsequent security management responsibilities shall be communicated in official Oxfam records including but not limited to employment contracts, job descriptions, terms of references, minutes of governing or executive body meetings, explicit instructions and delegations of line management, or official agreements and policies.

Informed Consent & Right to Withdraw

Via their respective line managers, employees shall be informed of the foreseeable risks related to their role and their place of work. By accepting the assigned duties after having been provided with relevant information, the employee is generally deemed to have provided their informed consent to accept these risks and the risk treatment[20] options and processes implemented by the employer.[21]

Employees may decline to undertake an assigned duty if their individual risk tolerance is lower than that of their employer. Likewise employees may withdraw from a location for the same reason. If withdrawing from a duty station for security reasons, employees shall immediately inform their line manager and as soon as practical record the reasons for the withdrawal. Such cases shall be subject to procedural review by the employer.

[19] **Risk owners** are the persons with the decision making authority and accountability to manage risks (ISO 31000/2009 & ISO Guide 73/2009)

[20] **Risk treatment** is defined as the process to modify risk. This may include measures to avoid, reduce, mitigate, and transfer risk, or a combination of these; (adapted from ISO 31000/2009 & ISO Guide 73/2009)

[21] The precise position may depend on the nature of the relationship between the employer and employee

Individual Obligations & Self Generated Risks

Oxfam employees are obliged to work with their employers to manage risks, and are responsible for taking reasonable and meaningful actions to manage their own safety and security. Individual behaviour is key to an employee's own safety and security as well as that of the organisation, co-workers and the effect on program objectives. It is very important that each and every employee accepts this responsibility, and understands that failing to adhere to security plans and other behavioural guidelines can put other people at risk. Negligent actions that create self-generated risks[22] are likely to lead to dismissal or other disciplinary action.

Gender and Security

Men and women can be, and often will be affected differently by specific threats. Likewise men and women may perceive or understand risk differently because gender influences an individual's vulnerability to certain threats. Oxfam's security policy recognizes gender as a potential vulnerability factor when assessing risks. Likewise gender may influence specific risk treatment options, and used to reduce the risk of harm (e.g. deciding to deploy or not deploy only men or only women to a certain context for a specific program objective). Risk assessments, local security management plans and subsequent risk treatment options shall explicitly communicate how gender is considered within the local context.

Non-Discrimination & Equality of Risk Treatment

A specific threat may produce different levels of foreseeable risk between different groups working in the same operating context. Oxfam's risk attitude and approach to security management is non-discriminatory and shall ensure risk treatment options produce (to the extent possible) equal protection for employees and associated personnel. This may require different risk treatment approaches, strategies, procedures or resources for specific individuals or groups even if these individuals or groups are working in the same operating context on the same program.ö

While risk treatment may sometimes appear unequal (e.g. different rules between national and international employees), the resultant level of acceptable risk is the intended outcome of a non-discriminatory approach to security management that aims to be applied without distinction or discrimination of any kind.[23]

Privacy of Information

Oxfam should act responsibly to ensure personal and other information is used, stored or disposed of appropriately, and should have regard to relevant regulatory requirements.. Local SMPs may also need to address privacy or data protection in terms of electronic networks, and/or hard copy files.

[format note – page break]

[22] **Self generated risk** is defined as the actions or inactions of a person or group resulting in risks that would not ordinarily be present in a given context

[23] Informed by the Universal Declaration of Human Rights, "non-discrimination" refers to the principle that no distinction of any kind applies, such as race, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Responsibilities

Individual Employees

Oxfam employees are responsible for:

- Complying with all security policies, procedures, directions, instructions, regulations or plans
- Taking care of their own safety and security and of the staff they manage
- Actively contributing to the development and maintenance of security management policy and procedures
- Ensuring their behaviour is in line with Oxfam's governing frameworks
- Reporting security incidents up and down their management line

Line Managers - Generic

Line managers are responsible for:

- Ensuring their staff and associated personnel have access to security management policies, plans and procedures
- Monitoring compliance to security policies, plans and procedures by their staff
- Reporting security incidents up and down their management line
- Identifying staff security training, learning and development needs and ensure access to the training (including appropriate planning and resourcing)
- Reporting organisational security management performance on a regular basis to governing bodies

Line Managers - Country Directors & Associate Country Directors

In accordance with the Oxfam Security Protocol, Country Directors and Associate Country Directors are **responsible for ensuring an appropriate security management system is in place** for their respective offices and/or programs. This obligation will involve a combination of the listed responsibilities for individuals, line managers and directors as contained in the policy and other governing documents. In addition Country Directors and Associate Country Directors are to work with the Country Leadership Team (where applicable) to ensure that minimum standards are met for program management, human resources, finance, security, and health and safety.

In addition to the above, Country Directors and Associate Country Directors are responsible for:

- Effectively delegating specific security management roles, tasks and functional responsibilities (whether to security-specific employees or others)
- Leading and managing the review and updating of local SMPs
- Contributing to establishing a local security information networks

Other Directors & Executive Officers

Directors and Executive Officers are responsible for:

- Ensuring full implementation of Oxfam's security policy
- Ensuring security management needs are identified and effectively communicated in program proposals and reports
- Ensuring adequate resources are made available to address security management needs
- Ensuring a crisis management process is developed, implemented, and periodically tested
- Holding line managers and employees to account for individual behaviours and attitudes towards security risk management

- Reporting on an annual basis to governing bodies (e.g. boards or councils, donors, etc.) Oxfam's security management performance

Security Working Group (SWG)

The SWG is a forum where Oxfam affiliates share security information, exchange ideas and discuss proposals to achieve a coordinated approach to security management.
The group is responsible for:

- Exchanging security information to encourage better security management practices
- Providing support and advice to line managers on the development of security procedures and plans for each country
- Coordinating and following up on Oxfam's participation to external security networks
- Agreeing on Oxfam's representation to international (European/UN/US) security networks
- Facilitating learning and exchange experiences
- Making proposals and recommendations regarding security management coordination within the collective Oxfam membership
- Coordinating with Oxfam security focal points (SFP) on security management issues

Governing Bodies (e.g. Boards, Councils, etc.)

Governing bodies are responsible for:

- Providing explicit governance and oversight of security management performance
- Holding directors and executive officers accountable for security management performance

Security Levels

Oxfam's security management actions shall be guided by assessing foreseeable risks in a given operating context. The overall risk shall be allocated a measurable security level[24] and the security levels shall be communicated in local security management plans, and be subject to regular review.

Security Management Plans

Security management plans (SMP)[25] must be available in all Oxfam offices. SMPs shall be subject to periodic review to ensure the information remains current. SMPs shall be accessible to all employees and associated personnel working in the operating context relevant to the plans. SMPs and all associated documents must be translated into the appropriate working language.

Security Incident Reporting

All security incidents, including minor incidents and near misses, must be reported immediately via line management or other locally defined reporting lines. Security incident reports shall be shared as widely as possible within Oxfam and its implementing partners,

[24] Refer to Annex C – Oxfam Security Levels Table
[25] Refer to Annex D – Oxfam Security Management Plan Template

and when appropriate, shared with others (e.g. United Nations organizations, other NGOs, local authorities, etc.)

Evacuation, Relocation & Hibernation

In the context of the Oxfam security policy, *"evacuation, relocation and hibernation"* are processes intended to move persons to a safer location, or remain in a sustainable safer location. Security management plans shall explicitly address evacuation, relocation and hibernation needs, relevant to the local context. Such plans will communicate decision-making authority (as reflected in other governing documents referenced in the policy), delegation of responsibilities, the criteria for which persons shall be moved and when, and the processes for evacuating, relocating and hibernating. In accordance with the Oxfam Security Protocol, Country Directors and Associate Country Directors of the managing affiliate are responsible for leading and managing evacuation, relocation and hibernation activities.

Implementing Partners

Partners are responsible for their own security management. If necessary Oxfam may assist partners to build their own local capacity to effectively exercise this responsibility. This assistance may include training, information sharing, mentoring, provision of security management resources, or a combination of these. Country Directors shall decide if assistance to partners is necessary, and the extent of any such assistance.

Oxfam shall consult with partners on context and risk analysis and share security management information with them (as appropriate to the local context). The partners are encouraged to report incidents to Oxfam. Oxfam will not expect implementing partners to work at locations that we consider too insecure or unsafe to work ourselves unless the risk transfer is clearly demonstrated as acceptable to both parties.

Use of Armed Protection

Armed protection is only compatible with Oxfam principles and programs in exceptional circumstances. Generally the use of armed protection is an absolute last resort option to reduce risk.

Oxfam's *Guidance Note: Obtaining Authorisation to Use Armed Escorts/Guards: An Exception to the OI Security Protocol (April 2011)* states:

> *"Exceptions to the protocol may be considered and authorised, according to the process outlined, when there is a compelling programme reason, when the threat is largely banditry, not political, when an acceptable provider is available and when the deterrent will be effective. Exceptions may be sought for a specific time period (if long-term, it must be reviewed annually at a minimum), for a specific project or for a specific one-off activity. However, in extreme and time critical situations, the use of armed escorts for emergency relocation and evacuation may be authorised by the most senior staff member present."*

Engaging with Armed Actors

Oxfam's relationships with armed actors are guided by the *SCHR Position Paper on Humanitarian Military Relations (January 2010)*. Oxfam will engage with any third party it

deems necessary in order to achieve stated programme objectives. At times this may include engaging (having indirect or direct contact) with armed actors.[26] Such contact with armed actors shall only be pursued after consideration of the associated risks and when it is reasonably assessed the desired outcomes will support programme objectives.

Crisis Management

The security policy aims to help reduce the likelihood of a crisis event affecting Oxfam's personnel or programs. Specific crisis management systems form part of Oxfam's overall security management approach, and are designed to address foreseeable events such as abduction or kidnapping.

As necessary Oxfam will develop and implement management systems to address context-specific issues that may present a crisis. Oxfam's crisis management systems include country-level crisis management plans[27] and although contextual, will aim for the following priorities and objectives:

Crisis Management Priorities:

1. Safety of employees and associated personnel
2. Reducing programmatic and operational disruption
3. Protecting Oxfam's reputation

Crisis Management Objectives:

1. Resume usual programs and operations as quickly as possible, or
2. Transition to an alternative means of programs and operations, or
3. End programs and operations in a given context

No Ransom or Other Concession

Oxfam does not pay ransoms, or concede to other demands from belligerent parties who threaten Oxfam employees or associated personnel. When appropriate, in serious incidences when employees are the victim of kidnap (or similar circumstance) Oxfam will support the work of relevant police forces (or other authorities) with the legal jurisdiction to act on such matters.

Training, Learning & Development

Oxfam will take continued actions to build the security management capacity of its global workforce.[28] Employees (and where assessed as relevant and appropriate, associated personnel) will have access to security-related training and professional development opportunities during their employment term as appropriate. Security management training strategies shall be determined and communicated to all relevant parties. These strategies must include an assessment of current security skills and competencies, gaps between current skills and those required due to assessed risks, resources, and explicit reference to budgets sufficient to meet training needs.

[format note – page break]

[26] Armed actors may include State military, police or other legitimate security forces; or non-state organized groups, or individuals.

[27] Refer to Annex E – Crisis Management Plan Template

[28] For more guidance refer to the *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*, Standard 4: Competent Workforce, p.14

Annex A: Oxfam Code of Conduct

Introduction

As one Oxfam (*any Oxfam Affiliate and / or Oxfam International throughout the world)* we are a strategic network of organisations working together internationally to find lasting solutions to poverty and injustice. We share a common vision, common philosophies and, to a large extent, common working practices. We all have the same brand values, the same passion and commitment. We have joined forces as an international confederation because we believe we will achieve greater impact by working together in collaboration with others.

Together we are working towards a world in which people can live with dignity, have their basic needs met and their basic rights respected, and have the ability to control their own lives.

As we work to achieve our ambition and vision of 'a just world without poverty' we should always remain true to our core mission, aims and values. This Code of Conduct will help you live by them by providing guidance in the face of ethical dilemmas you may experience. It shows you what to do when a situation is complex by providing standards and values for you to follow and how to protect against situations that may damage you or Oxfam. It also seeks to ensure that employees avoid using possible unequal power relationships for their own benefit.

The rules and guidelines contained in this Code of Conduct, together with your employing affiliate's policies and procedures and the terms and conditions of your employment (as outlined in your employment contract or your collective agreement if applicable), provides a framework within which all Oxfam employees, regardless of location, undertake to discharge their duties and to regulate their conduct. They also support Oxfam in our role in implementing, monitoring and enforcing these standards.

The Code does not exempt anyone and in accordance with the relevant employing affiliate's policies and procedures, any breach may result in disciplinary action (including dismissal in some instances), and in some cases could lead to criminal prosecution.

In accepting your appointment you undertake to discharge your duties and to regulate your conduct in accordance with the requirements of this Code, thereby contributing to Oxfam's quality of performance and reputation. The code describes what Oxfam expects from its employees and what the employees can expect from Oxfam.

Whilst recognising that local laws and cultures differ considerably from one country to another, Oxfam is an International Non-Governmental Organisation (INGO) and therefore the Code of Conduct is developed from International and UN standards.

This Code is subject to relevant international human rights law, wherever the employee is employed and shall be read in a manner that is compliant with that law.

Standards & Values

As an Oxfam employee I will:

1. Uphold the integrity and reputation of Oxfam by ensuring that my professional and personal conduct is demonstrably consistent with Oxfam's values and standards.

I will seek to maintain and enhance public confidence in Oxfam by being accountable for the professional and personal actions I take and ensuring that I manage the power that comes with my Oxfam position with appropriate restraint.

Whilst observing the requirements of the Code of Conduct, I will also be sensitive to, and respectful of, local customs and culture, even if the norms and values in that cultural context

differ from the Code of Conduct. I will if necessary seek (and will receive) support and advice from Oxfam.

I will not work under the influence of alcohol or use, or be in possession of, illegal substances on Oxfam premises, vehicles or accommodation.

2. Treat all people with respect and dignity and challenge any form of harassment, discrimination, intimidation or exploitation.

I will contribute to a working environment characterised by mutual respect, integrity, dignity and non-discrimination.

I will ensure that my relationships and behaviour are not exploitative, abusive or corrupt in any way.

I will respect all peoples' rights, including children's rights, and will not engage in any form of abuse or sexual exploitation of children (as defined in the country Child Protection Policy), or of any persons of any age.

With beneficiaries, I will not exchange money, offers of employment, employment, goods or services for sex nor for any forms of humiliating, degrading or exploitative behaviour.

I will use my best endeavours to report any such behaviour or malpractice in the workplace by others to my line management or through recognised confidential reporting systems.

3. Perform my duties and conduct my private life in a manner that avoids possible conflicts of interest with the work of Oxfam.

I will declare any financial, personal, family (or close intimate relationship) interest in matters of official business which may impact on the work of Oxfam (e.g. contract for goods/services, employment or promotion within Oxfam, partner organisations, beneficiary groups).

I will advise Oxfam of any intention to seek a nomination as a prospective candidate or another official role for any political party or public office to clarify whether any conflict, or perceived conflicts, with my duties with Oxfam may arise.

Even when the giving and acceptance of gifts is normal cultural practice I will reject monetary gifts or inappropriate gifts from governments, beneficiaries, donors, suppliers and other persons, which have been offered to me as a result of my employment with Oxfam. Where the giving and acceptance of gifts is normal cultural practice, I will ensure that such gifts are within the limits of reasonable judgements and in accordance with procurement policies and I will report gifts to the line management and where appropriate hand them onto Oxfam.

I will assure that assistance by Oxfam is not provided in return of any service or favour from others.

I will act against any form of corruption and not offer, promise, give or accept any bribes.

4. Be responsible for the use of information, equipment, money and resources to which I have access by reason of my employment with Oxfam.

I will use my discretion when handling sensitive or confidential information.

I will seek authorisation before communicating externally in Oxfam's name and will avoid any unintended detrimental repercussions for me or Oxfam.

I will appropriately account for all Oxfam money and property, (e.g. vehicles, office equipment, Oxfam-provided accommodation, computers including the use of internet, email and intranet).

5. Protect the health, safety, security and welfare of all Oxfam employees, volunteers and contractors.

I will undertake and act on appropriate risk assessments.

I will comply with local security management guidelines and be pro-active in informing management of any necessary changes to such guidelines.

I will behave in such a way as to avoid any unnecessary risk to the safety, health and welfare of myself and others, including partner organisations and beneficiaries.

6. Promote human rights, protect the environment and oppose criminal or unethical activities.

I will ensure that my conduct is consistent with the human rights framework to which Oxfam subscribes.

I will use my best endeavours to protect the natural environment and work in a sustainable way.

I will contribute to preventing all forms of criminal or unethical activities.

I will inform Oxfam of any relevant criminal convictions or charges I have had prior to my employment in which Oxfam may have a legitimate interest.

I will also notify Oxfam if I face any criminal charges during my employment that may impede my ability to perform the duties of my position subject to national legislation.

I will adhere to following policies and procedures (see list below) that support the above Standards:

- Child protection
- Anti harassment and bullying
- Disciplinary procedures

In accepting my appointment I undertake to discharge my duties and to regulate my conduct in accordance with the requirements of this Code thereby contributing to Oxfam's quality of performance and reputation.

Annex B: Oxfam Security Protocol

(As reviewed March 2014)

Vision

Oxfam recognises that working in complex environments may entail staff being present in insecure and violent contexts. Affiliates undertake to reduce the risk of operating in such environments by effective security management.

Close collaboration of Affiliates in the management of security will lead to effective and efficient programme delivery, as well as seeking greater safety and security of staff and assets. This protocol outlines the architecture by which this vision will be realised through provision of principles, standards and guidance.

The Oxfam Security Protocol is mandatory for all countries and all Affiliates.

General agreements

1. Staff safety and security is a higher priority than the protection of material assets, the preservation of programmes or the expression of advocacy objectives.
2. Affiliates recognise the impact that their staff behaviour, actions and programmes may have on Oxfam's overall reputation and brand, and hold each other accountable.
3. Security management is an integral part of programme management and as such subject to systematic and methodical discussion at all levels.
4. The right of individual staff to withdraw from insecure situations is supported by all Affiliates.
5. In our humanitarian work, affiliates work according to the principles in the Code of Conduct for The International Red Cross and Red Crescent Movement and NGOs in Disaster Relief.
6. Affiliates agree not to use armed guards and that staff will not carry or take up arms. However, the exceptional use of armed guards may be authorised by the Executive Director (ED) of the Managing Affiliate (MA), following a collective risk analysis[29] and decision by all Affiliates present. The ED will advise other Affiliate ED's present of the specific circumstances of the authorisation.
7. Affiliates agree not to make statements or undertake activities that could compromise Oxfam's standing as an independent party, based on Oxfam's policies and principles, and sign-off systems and procedures.
8. Affiliates will respect the confidentiality of what has been shared with them.

Global agreements

Affiliates must have a Global Security Policy and a Crisis Management Plan in place. The Oxfam Security Network Working Group monitors compliance on an annual basis, on behalf of the PDG.

The Global Security Policy should be proportionate to the Affiliates mandate, programme and mode of operation. It should clearly articulate the expectations the Affiliate has of its employees and the responsibility the Affiliate assumes on behalf of its employees.

[29] According to Guidance Note: Obtaining Authorisation to Use Armed Escorts/Guards: An exception to the OI Security Protocol

The Crisis Management Plan establishes arrangements and resources required to manage a critical security incident that is so complex or acute (such as kidnap) it cannot be managed adequately within the normal scale of operations. The plan provides a framework for necessary steps during such a crisis and its immediate aftermath.

Country level agreements

1. The MA Country Director (CD) in consultation with the Associate Country Directors (ACD's), and managers from other Affiliates present in that country, is responsible for ensuring an appropriate security management system is in place.
2. The system includes a countrywide Security Management Plan (SMP) (format in Oxfam Security Management Formats) that applies to everyone in country. The creation and maintenance of the SMP is a consultative, participatory and collaborative effort to ensure ownership and compliance. The SMP must be reviewed every year or more frequently if the security context changes significantly.
3. The process for the establishment and review of the SMP consists of the minimum following steps: consultation, drafting, formal feedback, approval, dissemination and communication. The most recent approved version must be posted on Sumus. After presentation of the final draft, Implementing Affiliates (IA) are given a reasonable period to provide feedback. The non-provision of feedback within the stated timeframe implies approval. Approval is given by the CLT, and subject to the MAs approval mechanism. The above process should be clearly documented in the CLT minutes.
4. As part of the SMP, the CD is also responsible for ensuring the development of security levels according to the agreed five levels system (format in Oxfam Security Management Formats). Although the security levels headings are fixed, the indicators and actions must be made context and risk specific. A security levels document must also be developed for field offices, which is specific to that particular context, and is approved by the CD.
5. Where possible the CD consults in order to set the appropriate security level. However, the CD has the express right to set the security level including the evacuation of staff for all offices. The decision is binding on all Affiliates and they must comply.
6. Lowering the security level is subject to the MAs mechanism as described in their security policy.
7. The right of Affiliates to withdraw from locations because of insecurity, prior to such a decision by the CD, is supported by all Affiliates.
8. Certain tasks may be delegated to an IA for practical reasons, but the responsibility cannot be delegated.
9. If field offices exist, location specific plans must be developed and maintained by the appropriate Affiliate. The CD ensures quality and consistency with the overarching countrywide SMP.
10. Each Affiliate is responsible for staff that they manage and is responsible for ensuring that staff and visitors comply with the security management system.
11. Affiliates share responsibility to feed into the security management system, including joint context analysis, risk assessment and risk mitigation measures.
12. Non-present Affiliates, wishing to visit a country, must have authorisation from the MA, and must abide by the authority of the MA and the SMP.
13. Affiliates must meet the minimum standards outlined in this document. Where Affiliates global security policy imposes other standards on specific issues, these may be met in addition to the minimum standards.

14. The CD is held accountable by their line manager, and the Programme Governance Group (PGG), and has the right and duty to report any concerns about the functioning of security management to the PGG chair.
15. Should Affiliates disagree about security management issues they take their concerns to their line management, who will deal with them bilaterally or take the concerns to the PGG.
16. If issues cannot be resolved by the PGG, they should be escalated to the PDG.
17. Despite the process outlined above; urgent decisions, such as described in point 5, may be taken by the CD and are binding. Escalation to PGG, PDG or bilateral line management may take place simultaneously, but the urgent decision is binding and applied immediately.

How to meet country level agreements

1. Context analysis and risk assessment must be undertaken jointly, and must be a collaborative, consultative effort.
2. The choice of security approaches (for example, acceptance, deterrence and protection) is based on joint context analysis and risk assessment.
3. Roles and responsibilities for security management must be defined and assigned to named individuals. A clear explanation of the relationship between the PGG, CD, and ACD's must be documented in the SMP.
4. Information is shared between Affiliates, and mechanisms to do so are institutionalised. The CD ensures that information is gathered from, and shared with, other actors (such as INGOs, UN, partners, local authorities and other stakeholders) and is crosschecked and analysed.
5. The security levels chapter of the SMP is developed in detail, including country specific indicators and relevant actions to take at each level. Specifically this will include definition of essential and non- essential staff.
6. The CD oversees security learning and development needs, and coordinates efforts to provide joint training initiatives.
7. Resources for managing security, including provision for learning and development, should be budgeted for.
8. The CD is responsible for ensuring the development of a current, agreed Welcome Pack (format in Oxfam Security Management Formats).
9. Incident reporting and analysis – in addition to meeting line management reporting requirements; all security incidents must be shared with all Affiliates. (format in Oxfam Security Management Formats)
10. Each Affiliate is responsible for ensuring security briefings are conducted and for monitoring the security of all their staff and visitors. The CD should be notified of all visitors and new staff.
11. Partners are responsible for managing their own security. Affiliates need to ensure that staff and partners are clear about their specific roles and responsibilities regarding security management.

Annex C: Security Levels

	Indicators	Actions
1	Normal: Situation calm Low level of crime	All staff aware of current security management plan General precautions against crime Emergency supplies in place (see evacuation plan) Evacuation plan in place
2	Precautionary: Situation less stable, higher risk of sporadic violence, possible threats against staff High level of crime Increased military presence Increased demonstrations	Contingency plans updated, staff aware of hibernation and evacuation sites Emergency supplies checked Higher security awareness by staff
3	Restricted Movement/Restricted Programme: Increase in tension Increased demonstrations, with violence and anarchy Indications that military/belligerents are mobilising Threats/demonstrations directed at International organisations Violence in project areas	Security updates every 2 days Staff movements restricted Programme activities may be partially suspended Hibernation/evacuation points agreed with other NGOs Curfew All incidents reported immediately No additional staff to travel into the country Eligible dependents may be evacuated
4	Partial Evacuation/Hibernation: Increased tensions and violence, including in locations near offices Increased violence in project areas Harassment/violence directed at International organisations Lootings Security forces unable to maintain law and order	Security updates daily/or more often Essential/low risk staff only to report to work Initiate evacuation/hibernation plan High-risk &/or non-essential international staff to evacuate Daily contact with line management Programme activities likely to be suspended
5	Office Closure and Suspension of activities: Unacceptable level of risk Direct threats/attacks on International organisations/staff and or property Inability to continue programmes Large-scale mobilisation of belligerents Indiscriminate violence, looting and destruction	Closure of office. See evacuation Plan Closure of all programme activities

Annex D: Security Management Plan Template

Front page: title, date, author and review date

Chapters:

1. Introduction: purpose and scope of the document and its relation to other documents. First principles such as right to withdraw, duty to contribute to security etc.

2. Context Analysis (summary)

3. Internal Analysis. An overview of the joint Oxfam program, including partner activities.

4. External Analysis. General analysis (history, gender, religion, culture, infrastructure, demographics etc) conflict analysis, crime analysis, actor mapping, incident mapping.

5. Risk Assessment; threat identification and analysis, vulnerability analysis, threshold of acceptable risk.

6. Security approaches: the balance between acceptance, protection and deterrence and an explanation of implementation methodology.

7. Roles and responsibilities.

8. Standard Operating Procedures (may include vehicle and travel, communications, personal behaviour, conflict survival, site protection etc).

9. Contingency Plans (may include hostage taking, sexual assault, gunfire, carjacking etc).

10. Evacuation Plan.

11. Incident reporting and analysis. (Definition of security incident, reporting structure, explanation of how lessons will be learned).

12. Security levels: built on the generic system of levels (section 4 of the security policy), a context specific overview describing the security levels, and related indicators and actions.

13. Annexes (contact numbers, maps, medical evacuation procedures, etc).

Annex E: Crisis Management Plan Template

Front page: title, date, author and review date

1. Introduction
2. What Constitutes a Crisis?
3. Management and Decision Making
4. Crisis Management Team (CMT)
    a. Immediate Actions of Crisis Director
    b. Immediate Actions of CMT
    c. In the Event of an Abduction
    d. Individual CMT Member Actions
5. Incidents Involving Oxfam Affiliates or Other Agencies
    a. Oxfam Affiliates
    b. Other Organisations
    c. Partners or Community Volunteers
6. Human Resources
7. Family Liaison
    a. Delivering the Bad News Message
    b. Family Liaison Contact
8. Communication
    a. Media Communications
    b. Internal Communications
9. Information Management
10. Emergency Operations Room (EOR)
11. Post Crisis
12. Analysis and Lessons Learned