Oxfam Security Policy

APPROVED by EDs 11 03 2014,
REVISED JULY 2018

Table of Contents

1 Introduction

Oxfam is an international confederation, working together with partners and local communities in more than 90 countries. Our vision is a just world without poverty, where people are valued and treated equally, enjoy their rights as full citizens, and can influence decisions affecting their lives. Our purpose is to help create lasting solutions to the injustice of poverty. We are part of a global movement for change, empowering people to create a future that is secure, just, and free from poverty. We use a combination of rights-based sustainable development programmes, public education, campaigns, advocacy and humanitarian assistance in disasters and conflicts[1].

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 Affiliates 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.[2] 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”. Where the term ´Affiliates´ is used, it refers to the different formal employers in the Confederation (including the Oxfam International Secretariat).

1.1 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 employees with strategy and direction 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.

Detailed practical guidance in implementing the policy and establishing and maintaining an effective security management framework are provided in the Security Management Toolkit[3].

1.2 Complementarity with other Governing Frameworks & Codes

Several governing frameworks guide Oxfam’s programme 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 is a signatory of or a member of.

The security policy is complementary to the following governing frameworks:

- Oxfam Code of Conduct[4]

[1] Oxfam mission statement,
[2] **Associated personnel** are persons who are not employees but who are engaged by Oxfam for the purpose of supporting or delivering the organisation’s programmes. Associated personnel may include volunteers, interns, consultants or official visitors.
[3] Oxfam Security Management Toolkit,
[4] Oxfam Code of Conduct

- EA Service Level Agreement[5]
- The Code of Conduct for The International Red Cross and Red Crescent Movement and NGOs in Disaster Relief[6]
- SCHR Position Paper on Humanitarian Military Relations[7]

Where necessary the governing frameworks are referenced in the policy. However, the complementarity noted above is not intended as a cross-referencing guide. 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.

1.3 Applicability and Policy Implementation

The security policy applies to Oxfam Affiliates, (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 programme or operational management activities.

1.4 Security Management Approaches

Security must be actively managed, not just planned for, and is most effective when fully integrated into programme management. Managers must ensure security of persons and programmes is given a high priority, through objective setting, the performance management cycle, work planning/scheduling and appropriate budgeting and other relevant management tools. Security management approaches are informed by an understanding of the local context and based on the outcomes of risk assessments. Generally, approaches are not mutually exclusive; the key is to adopt the right mix in any 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 actor, achieves this. This identity must be communicated clearly to all parties. The success of an 'acceptance' approach depends on many factors including employee behaviour, employee diversity, type, design and implementation of programmes, community participation, choice of partners and proactive creation and maintenance of relationships.

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 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), evacuation plans, equitable employee policies, 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*[8], 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.

[5] EA Service Level Agreement
[6] IFRC Code of Conduct
[7] SCHR Position Paper on Humanitarian Military Relations,
[8] Obtaining Authorisation to Use Armed Escorts/Guards

1.5 Risk Attitude & Risk Tolerance

To achieve our purpose, Oxfam uses a combination of rights-based sustainable development programmes, public education, campaigns, advocacy, and humanitarian assistance in disasters and conflicts. Almost any operational activity may present threats to personnel and assets. Guided by the humanitarian imperative, Oxfam's risk attitude[9] is aligned with our mission statement: to help create lasting solutions to the injustice of poverty. We are part of a global movement for change, empowering people to create a future that is secure, just, and free from poverty.

Oxfam will always assess and communicate the level of risk in any 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 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."*[10]

Risk assessments aim to provide information in sufficient detail in order for managers and other staff to take informed and effective security management 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 programmes
- The factors that expose or make Oxfam vulnerable to these threats
- The likelihood of a foreseeable threat occurring and the impact it may have on Oxfam's personnel and programmes
- The available options to treat the risks presented by these threats

Oxfam's tolerance[11] to take risks will always take account of programme objectives, the importance of what is to be achieved and the capacity to manage risks, as well as the impact of other strategic factors (e.g. key relationships, donor interests, etc.). Risk owners[12] will decide on a case-by-case basis whether the specific programme objectives and intended outcomes justify accepting the assessed level of risk.

Risks will be considered excessive where the likelihood of serious incidents is more probable than possible, taking into account the risk mitigation measures already applied. The risk threshold may be reached if, after

[9] **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)
[10] Red Cross Code of Conduct
[11] **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)
[12] **Risk owners** are the persons with the decision making authority and accountability to manage risks; (ISO 31000/2009 & ISO Guide 73/2009)

risks are analysed and assessed, the available mitigation measures are not adequate to reduce exposure to the high 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.

2 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.

2.1 Duty of Care & Security of Personnel

Security of personnel shall remain a higher priority than the protection of material assets, the preservation of most programmes, 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, managing security risks effectively according to Oxfam policy, managing security incidents and crises when they occur, seeking to ensure on-going care and post-incident care (e.g. counselling for victims, their families, and/or colleagues) is available to employees.

2.2 Risk Ownership & Delegation

Security management is a line management responsibility. 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."*

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.

2.3 Informed Consent & Right to Withdraw

Via their respective line managers, employees shall be informed of the foreseeable risks related to their duties or role and their place of work, as frequently as necessary, depending on the context. By accepting the assigned duties or role after having been provided with relevant information, as frequently as necessary, the employee is generally deemed to have agreed to accept these risks and the risk treatment[13] options and processes implemented by Oxfam.

[13] **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)

Employees may decline to undertake an assigned duty or role if their individual risk tolerance is lower than that of their line manager (the employer is not necessarily the one who will be determining the risk appetite, it will be OI/Line management), and/or if they feel that they are unsafe and/or if appropriate security management measures are not in place. 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. Usual HR processes will be followed as necessary.

2.4 Individual Obligations & Self-Generated Risks

Oxfam employees are obliged to work with their line managers and 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 programme objectives. It is very important that each and every employee accepts this responsibility and understands that failing to adhere to security plans and behavioural and management guidelines can put other people at risk. Negligent actions that create self-generated risks[14] are likely to lead to dismissal or other disciplinary action.

2.5 Equality of Risk Treatment & Diversity of Staff

Oxfam's risk attitude and approach to security management is non-discriminatory and shall ensure risk treatment options produce (to the extent possible) equal and fair protection for employees and associated personnel. However, a specific threat may produce different levels of foreseeable risk for staff working in the same operating context, due to an individual's diverse identity, e.g. gender, race, ethnic origin, physical and mental ability, sexual orientation, age, economic or social class, HIV/AIDs status, religion, nationality, family/marital status and political affiliation.

We recognise that also the infinite range of individual unique characteristics and experiences, such as communication style, life experience, educational background and other variables can influence personal perspectives. Identity can be a factor in perceiving or understanding risk differently, for example because of gender, and may make staff more or less vulnerable to certain threats. This may require different risk treatment approaches, strategies, procedures or resources for specific individuals or groups even for those working in the same operating context, on the same programme. 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 for application without distinction or discrimination of any kind.[15]

2.6 Privacy of Information

Oxfam employees must act responsibly to ensure personal and other information is used, shared, stored or disposed of appropriately, and must have regard to relevant regulatory requirements. Employees must be aware of the risks of sharing information and opinions on social media and other public sites, in addition they must follow sign-off procedures for sharing Oxfam information publicly. Local Security Management Plans (SMPs) may also need to address privacy or data protection in terms of electronic networks and/or hard copy files.

[14] **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

[15] 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.

2.7 Collaboration

Oxfam is committed to actively sharing security information and collaborating with other agencies for the collective security of all. Risk analysis needs to be undertaken and consideration given to making this possible in contexts where information may be perceived to be sensitive.

2.8 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 if employees are the victim of kidnap (or similar circumstance) Oxfam may support the work of relevant police forces (or other authorities) with the legal jurisdiction to act on such matters.

2.9 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.[16] 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.

3 Security Management

3.1 Security Management Toolkit[17]

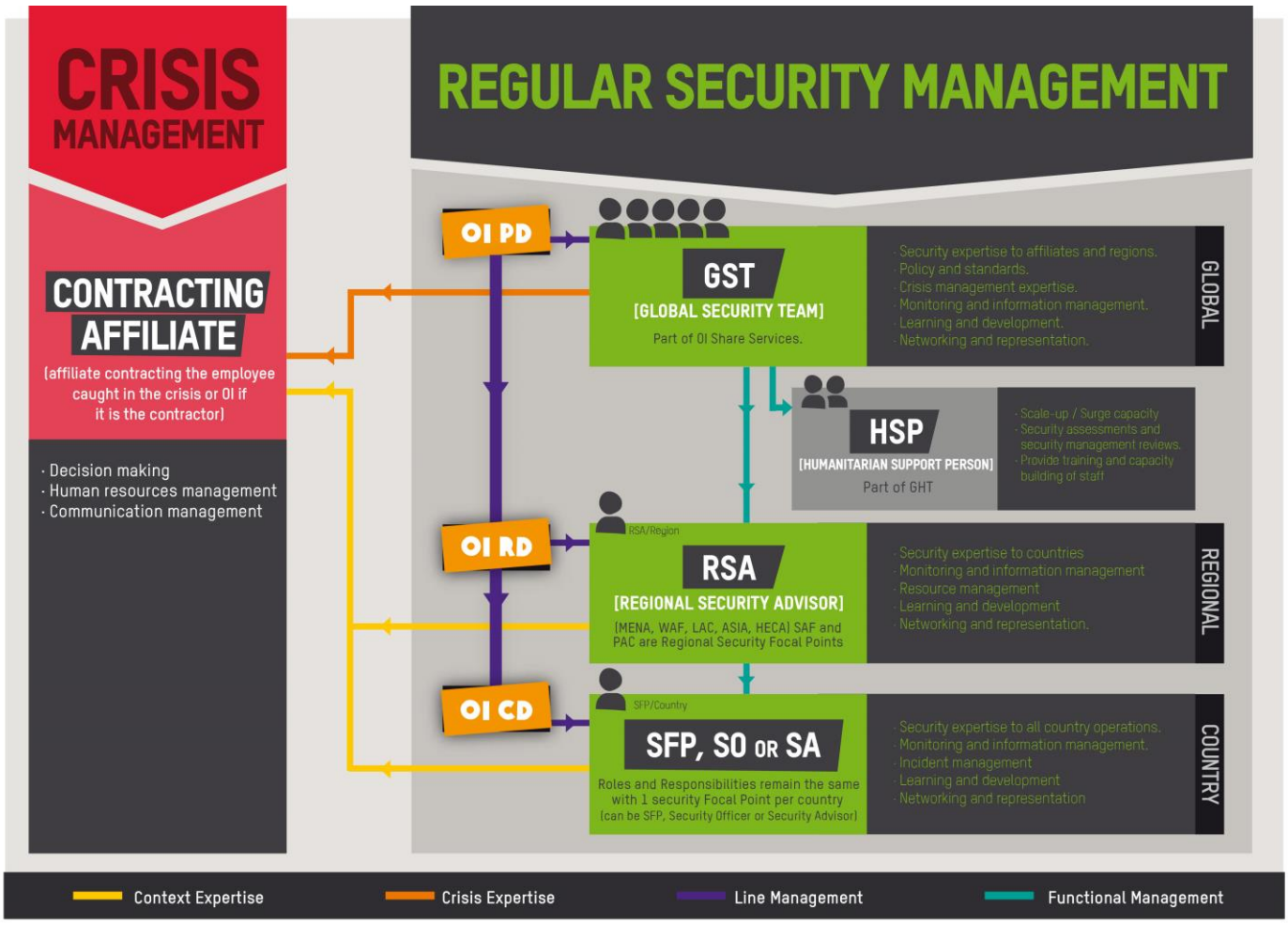
The Security Management Toolkit (STK) gives practical guidance to staff with security management responsibilities, to help establish an effective security management framework within all Oxfam programmes and operations. The toolkit supports staff to ensure that the Security Policy is consistently applied and implemented throughout the organisation. The Toolkit addresses the different security contexts in which Oxfam operates, and provides guidance on the wide range of security management issues and challenges that currently confront Oxfam programmes, partners and staff. In addition, the Toolkit provides a common set of security management tools and resource materials.

3.2 Security Management Structure

The Security Management Model is based on the following key concepts:

- Country Directors are responsible for ensuring an appropriate security management system is in place in their respective countries. RD and PD make them accountable for security management in countries
- Technical and advisory support will be provided by Regional and Global Security Advisors
- In the event of a security crisis situation the affiliate contracting the employee caught in the crisis will have an enhanced management role
-

[16] Armed actors may include State military, police or other legitimate security forces; or non-state organized groups, or individuals.
[17] Security Management ToolkitSecurity Management Toolkit ,



3.3 Responsibilities – Regular Security Management

❖ ***Individual Employees***

Oxfam employees are responsible for:

- Complying with all security policies, procedures, directions, instructions, regulations or plans (including required Security training)
- Seeking approval for visits to country and/or regional offices and compliance with security directions and requirements determined by the Country Director of the country they are travelling through, to or in
- Applying common sense in order to ensure their own safety and security
- 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 employees and associated personnel have access to security management policies, plans and procedures
- Managing risks and incidents (capacity, judgement, decision making etc.)

- Monitoring compliance to security policies, plans and procedures by their employees
- Reporting security incidents up and down their management line
- Identifying employees' 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

❖ ***Country Directors***

Country Directors are responsible and accountable for ensuring an appropriate security management system is in place for their respective offices and/or programmes. This obligation will involve a combination of the listed responsibilities for individuals, line managers and directors as contained in this policy and other governing documents. Country Directors must work with the Country Management Team (where applicable) to ensure that the Minimum Standards in Security Management (Security Management Toolkit)[18] are met.

In addition, Country Directors are also responsible for:

- Effectively delegating specific security management roles, tasks and functional responsibilities (whether to security-specific employees or others)
- Authorising travel to their country
- Setting standards for security training
- Ensuring security management is resourced and budgeted for and is a key consideration in the programme management cycle
- Leading and managing review and updating of the SMP
- Contributing to establishing local security information networks
- Ensuring that security is included in country learning and development plans

❖ ***Regional and Global Security Management***

Above country security management, support and technical advice will be provided by security positions in regional platforms and the Global Security Team.

The Regional Security Advisors support the security lead in each country to ensure that the country security strategy is developed, implemented, monitored and reviewed consistent with Oxfam policies, standards and requirements and supports the Regional Director to fulfil their management responsibilities.

The Global Security Advisors will support Oxfam with security and crisis management expertise, strategic policies, setting security standards in the confederation, networking and representation.

❖ ***Other Directors & Executive Officers***

Directors and Executive Officers are responsible for:

- Ensuring implementation of Oxfam's security policy
- Ensuring the risk tolerance is evaluated, especially in rapidly changing contexts
- Ensuring security management needs are identified and communicated.
- Ensuring adequate resources are made available to address security management needs
- Ensuring a crisis management process is maintained, implemented and periodically tested
- Holding line managers and employees to account for individual behaviours and attitudes towards security risk management

[18] Oxfam Minimum Standards in Security Management

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

❖ ***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 to account for security management performance

3.4 Responsibilities – Crisis Management

Good security risk management practice aims to help reduce the likelihood of a crisis event affecting Oxfam's personnel or programmes. Specific incident and crisis management systems form part of Oxfam's overall security management approach, and are designed to address foreseeable events that require higher than normal management support. This may include, but is not restricted to, abduction or kidnap.

Oxfam has a layered approach to incident and crisis management:

❖ **D*ay to Day Incident Management***

- It is the responsibility of line management to respond and manage day to day incidents
- The Oxfam Incident Management Plan (IMP) must be used to provide structure and support to incident management that requires a higher than normal level of management support
- The OI Program Director will, in consultation with the OI CD/OI RD and/or EA PD (or equivalent of PD holding duty of care responsibility for the affiliate), decide if and when incident will be classified a crisis

❖ ***Crisis Management***

- The Affiliate contracting the employee caught in the crisis will have an enhanced management role and will lead the Crisis Management Team (CMT) using the Oxfam Crisis Management Plan (CMP)
- The CMP details the process for deciding if an incident is a crisis and which Affiliate should lead if multiple Affiliates are involved.
- The IMP is designed to work within the structure of the CMP

3.5 Training, Learning & Development

Oxfam will take continued actions to build the security management capacity of its global workforce. 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.

Country offices must ensure that staff have the necessary security skills and awareness to enable them to stay safe in their particular operating environment. All staff must undergo an Oxfam security induction at the beginning of their employment, as part of their general induction and all staff who are based in country programmes, or who travel to country programmes, require online basic personal security awareness training (IFRC Stay Safe – Personal Security applicable to all staff and IFRC Stay Safe – Security management applicable to all managers). A more advanced level of intensive personal security training may be required for specific contexts.

CDs will determine whether intensive personal security training is mandatory for their country, as part of the country security risk analysis and risk treatment process. They must ensure that training is adequately budgeted for and that requirements are complied with.

Security management training strategies shall be determined and communicated to relevant parties. These strategies should 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.

3.6 Security Levels[19]

Oxfam's security management actions shall be guided by assessing reasonable foreseeable risks in any given operating context. The overall risk shall be allocated a measurable security level and the security levels shall be communicated in security management plans and be subject to regular review. The security level will help with the understanding of the volatility of the context and define the applicable minimum security standards accordingly.

3.7 Security Management Plans[20]

Security management plans (SMP) must be available in Oxfam offices and shall be subject to annual review or more frequently if the context changes significantly, 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 and stored in the country SMP Box folder.

3.8 Security Incident and Regular Reporting[21]

All serious security incidents, which result in harm, must be reported immediately, via line management or other locally defined reporting lines and followed up in writing within 24 hours. Minor incident and near missed should also be reported, including in writing.

Security reports should be shared as widely as possible with implementing partners and when appropriate, shared with others (e.g. United Nations organizations, other NGOs, local authorities, etc.).

A security incident is any situation, event, or incident that has caused, or could result in harm to Oxfam staff or associated personnel; significant disruption to programmes and activities; substantial damage or loss to Oxfam's property; substantial damage to the organisation's reputation.

[19] Oxfam Security levels
[20] Security Management Plan Template
[21] OSIRIS, Oxfam Security Incident Reporting Information System

3.9 Relocation, Evacuation & Hibernation

In the context of the Oxfam security policy, *"relocation, evacuation 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 relocation, evacuation and hibernation if these needs are 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 relocating, evacuating and hibernating.

3.10 Implementing Partners

Partners are responsible for their own security management. If it considers it appropriate, 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 may consult with partners on context and risk analysis and share security management information with them (as appropriate to the local context). 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, through our risk assessment, unless the risk transfer is clearly demonstrated as acceptable to both parties.

3.11 Use of Armed Protection

Employees may not use armed protection directly or indirectly and will not carry or take up arms. Armed protection is only compatible with Oxfam principles and programmes in exceptional circumstances, and may only be authorised by the OI PD, following a risk analysis must be footnoted to the specific risk analysis template same as footnoted on page 5 presented by the CD endorsed by the RD and after consultation of the GST

Oxfam's *Guidance Note: Obtaining Authorisation to Use Armed Escorts/Guards: An Exception to the Oxfam Policy* states:

> *"Exceptions to the policy 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 employee member present."*