RedR Global Safety & Security Policy

1. Purpose

This document sets out the global policy for the safety and security of RedR Australia personnel by:

a) Defining the safety/security management position and principals of the organisation, applicable to all RedR personnel and programmes, at all times;
b) Defining roles and responsibilities in relation to safety/security management at all levels;
c) Defining and presenting a summary of RedR's approach to managing safety/security and thus upholding its Duty of Care (DoC).

2. Scope

This policy applies to all RedR Australia personnel, including nationally and internationally recruited staff, deployees, consultants and all official visitors; this policy does not apply to other members of the RedR International family, unless they meet one of these criteria.

3. Policy Statement

It is recognised that the work of RedR often places great demands on personnel in conditions of complexity and risk. As a responsible agency RedR Australia has a DoC towards its personnel and takes all reasonable steps to minimise and manage the risks associated with its mission to ensure staff security and wellbeing.

Furthermore, robust safety/security management should not be viewed as abstract to effective programming. RedR Australia recognises that good organisational safety/security systems are critical to the effective implementation of programmes. As such the organisation seeks to ensure that sound risk management principles are mainstreamed throughout its operations.

4. Principles

In line with the organisation's core values of Empathy, Accountability, Collaboration and Integrity, RedR Australia's DoC management will be guided by the following principles:

4.1 Empathy with humanitarian causes, principles and beliefs:

4.1.1 Humanity. RedR Australia's mission, "To build resilience and relieve suffering in times of international crisis," necessitates deployment of personnel to potentially insecure and dangerous environments. Despite efforts to mitigate risks, some residual risk may ultimately remain; both organisational risk appetite and mission criticality will inform the extent to which a given activity proceeds despite this residual risk.

4.1.2 Engagement. The organisation will engage with risk in a proactive, managed and diligent manner, and with the belief that effective risk management enables access, not constrains it.

4.2 Integrity of operations:

4.2.1 Professionalism. All RedR staff and consultants are professionals who represent the organisation. They are bound by the RedR Code of Conduct, and are expected to comply with all safety/security-related requirements of their work and of the organisation.

4.2.2 Perspective. Safety and security management should acknowledge the following order of priorities:

1. Protect human life
2. Minimise trauma
3. Protect reputation (organisation, host agency and individual)
4. Protect information
5. Protect equipment and other physical assets

4.3 Collaboration internationally and locally:

4.3.1 Openness. RedR Australia believes in the triangulation of risks/threats that involves reliance on external partners for contribution to security assessment and procedures. Working closely with these external partners optimises safety. RedR will aim to share information and collaborate, where possible, with other members of the humanitarian community.

4.3.2 Acceptance. Acceptance plays a significant role in humanitarian safety and security management, and as such will always be the risk management approach of choice. Local acceptance depends on maintaining the upmost respect for native law, customs, culture, religion and beliefs. While working for RedR contextually-appropriate behaviour is required and expected.

4.4 Accountability to beneficiaries and to staff:

4.4.1 Enablement. Good safety/security management is an 'enabler', allowing RedR to operate even in hostile environments. All safety/security management should consider what is necessary in order to enable programmes to be safely carried out, and should be proportionate according to the risk.

4.4.3 Diligence. Security documents should be reviewed on an annual basis by the designated author or owner, or more frequently fluid security environments. Robust incident reporting protocols should identify areas for learning and improvement, and contribute to a culture of continuous improvement.

5. Procedures

5.1 Insurance. RedR must purchase and maintain sufficient and appropriate insurance to cover all personnel globally during their contracted engagement with RedR.

5.2 Third party due diligence. RedR can never delegate its DoC. Decision-making with regards to hosted (e.g. UN agency, foreign governments) deployments must take this into account, and may require host agencies to disclose certain information.

The annexed 'Due Diligence Process Map' and example forms document the process for capturing relevant information, which will include:

- Overview of host organisation and areas of programming and operation.
- A synopsis of key threats and (recent) risk events.
- Overview of working arrangements and office security
- Evidence of systems for hibernation, relocation and evacuation.

Failure to be able to provide some or all of this information does not automatically preclude working with a given partner, but should raise concern. In such cases, RedR should request further information, and/or implement specific protection and mitigation measures in order to ensure the security of its personnel and assets.

5.3 Risk Assessment. RedR will maintain a consistent and transparent means of quantifying risk. This is detailed separately in the Risk Management Policy.

5.4 Selection. RedR will ensure that only personnel with the requisite skills and experience are selected to undertake a given role or posting. Where the evolving demands of a given role or posting change to be beyond the capability of a given individual, suitable training and/or other support/contingencies will be enacted to ensure that personnel are matched to situation.

5.5 Training and briefing. All personnel will receive a safety/security briefing as part of their employment induction where appropriate, which will be documented. All personnel will also receive appropriate safety/security training as required by a risk assessment conducted for any overseas trips and/or locations of employment.

Any personnel visiting a RedR Australia regional office will receive an adequate and documented briefing on location-specific security plans on arrival. In other locations where RedR does not have an office, a suitable alternative will be arranged; this may involve a security briefing from partners or from a visiting RM.

5.6 Field mission travel. RedR will maintain adequate procedures to (amongst other things) assess risk, approve and monitor the international, regional and in-country travel of RedR personnel. The MS&R must approve all international staff travel to higher threat locations.

5.7 Incident response. RedR must maintain a 24-hour emergency phone system, manned by an identified member of RedR Australia staff in Melbourne HQ. This number must be available to all personnel and Regional Offices. In the event of a critical incident, staff must be able to directly contact the identified staff member in Melbourne at any time. Melbourne HQ will work closely with RMs as required, however it should be clear that command and control of an incident will generally originate from Melbourne.

5.8 Incident reporting. A procedure for the recording of all risk events, including 'near misses' will be maintained by the MS&R. Analysis of incidents is critical to the operational learning and ongoing safety/security and risk management of the organisation. Incident reporting should take place in line with the relevant RedR policy.

5.9 Critical event management. RedR must maintain and regularly exercise an incident response plan, including details on the selection and training of an Incident Response Team (IRT). The IRT will assume ultimate decision-making authority during any critical event. In order to avoid confusion, it is imperative that the IRT maintains clear lines of communication with the relevant RM whenever assuming this authority.

5.10 Evacuation/Relocation. RedR can require staff to leave an area or impose other security measures if it is deemed necessary. This can be done by the MS&R (primary) or DSP (secondary) in Melbourne or the RM, with action to be taken in deference to the BAU 'chain of command'. For example:

- The MR&S or DSP may order the evacuation/relocation of all relocatable staff, even if the RM considers the situation workable.
- The RM may order the evacuation/relocation of local personnel even if the team considers the situation workable.

If an evacuation is declared, staff have no right to remain. If they chose to stay despite instructions from management, they may have their contracts terminated and insurance invalidated.

Decisions to evacuate/relocate cannot be taken unilaterally without consultation of the MR&S and/or DSP, unless the delay caused by so doing poses unacceptable additional risk(s).

5.11 Office security. A Security Management Plan (SMP) should exist for each RedR office. The MS&R is the ultimate owner of the SMP, though this may be delegated to RMs in the case of regional offices. RMs are to ensure it is regionally implemented and regularly reviewed for contextual currency. All visiting personnel must be fully briefed on the contents, practical application and authority of the plan; this is again the responsibility of the RM.

The SMP should follow published[1] and/or generally accepted best practice. Elements such as maps, travel/transport advice, site security and evacuation/relocation plans should be considered mandatory. Care should be taken to ensure SMPs are brief and succinct documents. Security plans should be developed in a collaborative manner, gathering as much input from staff as possible.

Where regular travel is expected to specific areas in country or to neighbouring countries this should also be taken into account in the plan. Country SMPs must capture contingency planning for medical evacuation; whilst RedR has access to the services of a retained medical assistance provider (ISOS), SMPs should include local provisions to be used in the

[1] 'Operational Security Management in Violent Environments', *Good Practice Review No. 8* (van Brabant 2010).

event evacuations are to be managed directly. This also follows the maxim that self-evacuation will often be the most efficient course of action.

5.12 Data handling and privacy. RedR will have access to sensitive security, HR and beneficiary information which must be kept confidential and safe. Managers must take this into account and have procedures for the safe storage, transmission and destruction of sensitive information both in HQ and Regional Offices in accordance with all relevant organisational policies and local/regional legal frameworks. This aside, any exposure of personal information should be governed by necessity, with care should care taken to minimise unnecessary exposure and/or discussion where not task/mission critical.

All computers and servers must be password-protected; this will be overseen by maintenance of an appropriate resourced and skilled IT provider.

6. Responsibilities & Reporting

6.1 All personnel. All personnel, regardless of seniority or experience, have a personal responsibility for their own safety and security. Each individual is obliged to:

- Actively participate in, and contribute to, the maintenance of safety/security measures, the awareness of safety/security risks and team safety/security.
- Understand and adhere to safety/security measures, as stated in their contract of employment, job description, country security plan, the RedR Code of Conduct and other policy documents, or as requested by the line manager or persons responsible for implementation of safety/security procedures.
- Be responsible for their own safety/security and that of the staff they manage, and behave as a positive representative for RedR (as per the RedR Code of Conduct).
- Report any actions or behaviour that breaches policy or jeopardises team safety/security.

6.1.1 National staff. Nationally recruited staff will not normally be evacuated across international borders. They will be included in localised relocation and hibernation plans as appropriate. In the event of an evacuation, best efforts will be made to relocate nationally recruited staff, working outside their usual home environment, to a place of safety within the country concerned. Location-specific security plans should contain information relevant to nationally recruited staff in the event of instability or incident leading to international staff evacuation.

6.1.2 Individual right to decline travel. Whatever RedR's risk assessment of a particular situation, any personnel who do not feel safe or secure have the right to decline to enter, or decide to leave the area of operation, by a method agreed with their manager and facilitated by RedR. In this case RedR will seek to identify an alternative position for staff members but reserves the right to terminate contracts if an alternative position cannot be identified. The line manager can over-rule this only in exceptional circumstances, for example, when the process of relocation or evacuation[2] is clearly more dangerous than staying.

[2] Relocation is defined as the movement of staff within a country. Evacuation is defined as the movement of staff across an international border.

6.2 The Board. The RedR Australia Board has the ultimate responsibility for safety and security of RedR staff, volunteers and consultants. The Board delegates operational responsibility to the CEO. It is the duty of the Board to satisfy themselves that the CEO has maintained his/her responsibility in these matters.

6.3 CEO. The CEO is the 'Risk Owner' for RedR Australia, and is supported in this with input from the RedR Senior Management Team (notably the Director Strategy & Partnerships) and the Manager Strategy & Risk. The CEO may delegate the management of safety and security as appropriate, while maintaining overall responsibility.

6.4 Director Strategy & Partnerships (DSP). The DSP has a specific responsibility to ensure RedR Regional Offices have security management procedures in in place, in accordance with this policy. This task may be delegated to the Manager Risk & Strategy, however the overall responsibility remains with the DSP.

The DSP is one of only two people (the other being the Manager Risk & Strategy) with permission to adopt practices that deviate from the policy.

6.5 Manager Strategy & Risk (MS&R). The MS&R has the delegated responsibility for this policy, its regular review (as a minimum annually) and ensuring its implementation at all levels. He/she also acts as the conduit between different RedR Australia teams and the DSP on matters of security and risk. This includes:

- Support to all RedR Australia functional areas, including as an initial point of escalation for any safety or security related concerns;
- Support to RMs;
- Support on organisational security, including review of RedR policy and processes according to best practice;
- Liaison with the Senior Humanitarian Trainer(s) responsible for security training to ensure that training practices are reflective of the extant threat environment;
- Other briefing and monitoring responsibilities including context scanning, information management, provision of safety and security advice, and the review of travel plans and risk assessments to high risk destinations.

The MS&R is one of only two people (the other being the DSP) with permission to adopt practices that deviate from the policy.

6.6 Regional Managers (RMs). RMs have responsibility for RedR Australia's operations in a particular country. They are responsible for safety and security management of all staff and official visitors to their country of operation, in accordance with this policy, and by default are the Security Focal Point. The RM is the ultimate owner of the Security Management Plan, and that all staff are aware of the security measures in place. If necessary, security documentation should be translated into the local language.

6.7 All Managers. Every manager (someone who has line management responsibility for other staff members) has responsibility for the security of the staff they manage, and in turn is under the responsibility of their own line manager.

7. Definitions

Approval pathway means the pathway through which a policy must proceed in order to be approved.

Board means the Board of Directors.

Key stakeholders means persons, or a class of persons, whose roles or responsibilities are directly affected by a policy and includes policy approvers and relevant process owners.

Major amendment includes a change likely to impact on:

(a) Objectives of the policy and/or
(b) Any requirement for implementation related to a decision or action of a key stakeholder

Minor amendment includes a change not likely to impact on:

(a) Objectives of the policy and/or
(b) Any requirement for implementation related to a decision or action of a key stakeholder
(a) A formal statement of principle that regulates RedR operations and
(b) An instrument approved under this framework

Process means the group of activities and tasks undertaken by staff to achieve a consistent output.

8. Related policy and documents

Duty of Care Information Capture
Duty Policy
Incident Reporting Policy
Incident Response Handbook
Interstate and International Travel Policy
Privacy Policy
Risk Management Policy

A. Due Diligence Process Map

9. Document control

Reviewed by:	S&R Manager
Approved by:	S&P Director
Review date:	1st April 2019
Next review:	1st April 2020
Distribution:	Internal only
Version number	2.0