Security plans

Security plans are key country-level documents that outline the security measures and procedures in place, and the responsibilities and resources required to implement them. Security plans should be established in all locations where your organisation has a significant presence or is regularly engaged. Even in situations where your organisation has no fixed presence but staff regularly visit, or where you have a single representative or small team, a basic document outlining security arrangements and emergency procedures will help ensure that staff understand the measures in place and, most importantly, adhere to them.

If the risk assessment identifies a threat, the security plan must advise staff on how to manage the risk from that threat.

Security plans must remain relevant and accessible documents, should address the specific risks that exist in that location, and, if appropriate, be specific about to whom and where the measures apply, for example, particular ethnic groups in specific regions. Plans should be updated regularly, especially following significant incidents or changes in the operating environment or activities. They should be translated into local languages where necessary.

Country security plan

Key components of a security plan for a country, or specific geographical area, should include:

- **Critical information** – a one-page summary of pertinent information for easy access and quick reference, for example, any restrictions such as curfew times or no-go areas, and important contacts.
- **Overview** – the purpose and scope of the document, who is responsible for the security plan, the organisation's risk attitude, date of completion and review date, and a summary of the organisation's security strategy/policy.
- **Current context** – a summary of the current operating context and the overall security situation, the main risks to staff, assets and programmes (risk assessments system), threats faced in this context, and evaluation of threats and rating of risk.
- **Standard Operating Procedures (SOPs)** – simple and clear security procedures that staff should adhere to in order to prevent incidents, and how to respond should problems arise. SOPs should be linked to the key risks identified and address issues such as cash in transit, communications, incident reporting, field travel and vehicle safety, facilities and site security, office and facility access control, robbery, vehicle accident, personal conduct, staff health and welfare, and information security.

- **Health and safety** – staff protection from health threats as well as accidents, stress and post-traumatic stress disorder.
- **Human Resources** – policies related to recruitment, background checks, contracts, confidentiality, inductions, risk assessment of roles, etc.
- **Security briefings** – what information should be provided to new staff and visitors, and when this information should be provided.
- **Administrative and financial security** – policies for preventing theft, fraud and corruption, as well as cash handling and procurement.
- **Security levels** – the organisation's security levels/phases, with situational indicators that reflect increasing risks to staff in that context and location, and specific actions/measures required in response to increasing insecurity.
- **Incident reporting** – the procedures and responsibilities for reporting security-related incidents, for example, the type of incidents to be reported, the reporting structure, and the format for incident reporting.
- **Crisis management** – members of your crisis management team and activation rules. Include contingency plans in anticipation of foreseeable threats or critical incidents, such as the relocation or evacuation of staff, natural disasters and medical emergencies.
- **Annexes** – additional information, documents and checklists to assist staff in implementing the procedures and plans, for example, contact lists, briefing checklist, and incident reporting form.

Ensuring staff affected by the risks are involved in preparing the security plans will increase the likelihood of them being adhered to because staff will then understand the why rather than just the what.

Further information

'Country Security Plan Example' by InterAction

'Module 6: Security plan' in EISF guide 'Security to go'