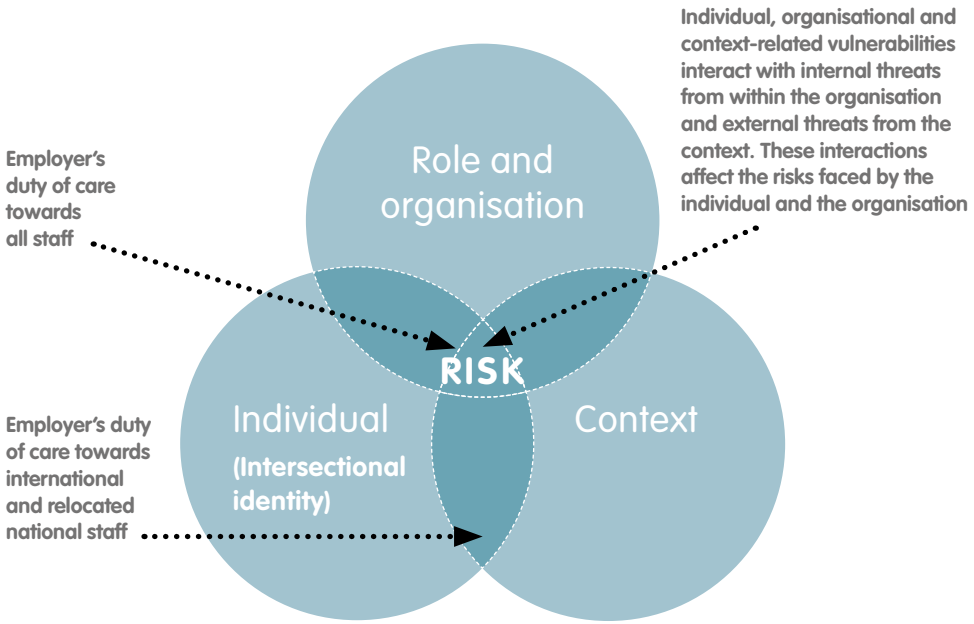
Inclusive Security Risk Management

An aid worker's personal security is impacted by the interplay between where the aid worker is, who they are, and their role and organisation. As employers, aid organisations have a duty of care to take all reasonable measures to protect their staff from foreseeable risks, including those that emerge due to an aid worker's personal characteristics – for example, biological sex, gender, ethnicity, cognitive and physical abilities, and sexual orientation.



A better understanding of the interplay between the different facets of an aid worker's identity can help an organisation understand the security risks faced by staff. The strength of adopting this holistic approach to identity is that it shows how different strands of power, identity, ability and choice intersect to influence the conditions in which aid workers live and work.

All aid workers have a diverse profile brought about by the intersectionality between the different aspects of their personal identities. This intersectional personal identity interplays with an individual's organisational role and their relationship to their operational context.

Individual Intersectional identity	**Organisation**	**Operational context**
Age	Seniority	Legal (national laws and their enforcement, including lack of protections)
Race/Ethnicity	Contract type (e.g. employee/consultant; local/international)	Cultural attitudes
Nationality	Contract duration	Rural/Urban/Regional differences
Religion	Job title	Bilateral agreements with employees' country of citizenship
Gender/Sex	Travel obligations	
Sexuality	Accommodation	
Physical/Mental health and ability	Partnership organisations	
Marital/Partnership status	Post relationship with external actors (e.g. government)	
Physical appearance	Organisational culture	
Previous professional experience	Organisational mandate	

The failure to understand how personal profile characteristics impact personal security can have implications for the security of both the team as a whole and for the individual aid worker, as well as causing serious security, legal and reputational issues for employing organisations.

Click on each box for a list of key recommendations or see pages 3-7 for the full list.

KEY RECOMMENDATIONS

Policy

- Make reference to staff diversity and the impact personal profiles can have on security in the organisation's security policy. Establish guiding principles on what this means for the organisation in practice.
- Keep the security policy up to date and reflect learnings from staff and incidents, as well as changes in legislation.
- Make clear links between the security policy and the equality, diversity and inclusion policy.
- Consult minority profiles in the development of policies, as this is an effective way to better ensure these policies will be inclusive.
- Complement policies with staff training and monitor implementation.

KEY RECOMMENDATIONS

Roles and responsibilities

- Clarify roles and responsibilities in relation to security and diversity as part of the organisation's security risk management framework.
- Consider providing specific training to security staff on duty of care and anti-discrimination obligations.
- Encourage security focal points to draw on external expertise where necessary to make appropriate security decisions that relate to personal risk profiles.
- Include HR teams in the security risk management planning process to offer legal guidance on anti-discrimination and reasonable adjustments, as well as to ensure staff wellbeing and duty of care are considered.
- Ensure that security and HR departments work closely together on security and diversity issues.
- Consider how to diversify representation in senior leadership at HQ and country levels and on boards of trustees.
- Ask senior leaders to act as role models to change organisational culture in relation to minority profiles, and to successfully lobby for change in attitudes towards diversity within the sector more broadly.
- Provide equality and diversity training for existing senior leadership and boards of trustees.
- Consider creating an equality, diversity and inclusion focal point to provide staff with a number of paths to raise concerns.
- Ensure that a diverse range of aid worker personal profiles are involved in security risk management processes and systems.

KEY RECOMMENDATIONS

Risk assessments

- Include a variety of specific profiles in the risk assessment to provide sufficient information for informed consent during recruitment and deployment.
- Collect information on staff profiles at recruitment stage in a systematic way that ensures data protection.
- Use this information to carry out inclusive risk assessments, which should include both internal and external threats to staff.
- Involve staff with a diverse range of personal profiles to develop risk assessments.
- Use these inclusive risk assessments to inform:
  - Job descriptions and recruitment packages
  - Briefings that aim to ensure informed consent of staff
  - Trainings
  - Other security risk management measures, e.g. mitigation activities and contingency plans
- Ensure inclusive incident reporting feeds into risk assessments.
- Respond to issues of staff mistrust in confidentiality and data protection – especially around dealing with internal threats.

KEY RECOMMENDATIONS

Security plans

- Consider internal as well as external threats in security plans.
- Include a broad cross-section of staff, national and international, in the security planning process, to understand a broad range of risks and the interplay between different facets of identity within the context.
- Ensure that while mitigation measures consider staff diversity, they remain similar for all staff whenever possible.
- Check that if differentiated measures are necessary for particular profiles, they are also proportionate to the specific risk.
- Involve affected staff in discussions around the specific mitigation measures to ensure their appropriateness and compliance.
- Provide training and support to empower security focal points and other decision-makers in managing internal threats to staff in collaboration with HR.
- Share security plans with staff at pre-departure stage, to allow them to raise concerns about particular risks, and provide more time to put in place proactive measures to address risks for staff with particular vulnerabilities.
- Consider the impact of digital security risks on staff as part of the organisation's security plan.

KEY RECOMMENDATIONS

Induction, pre-departure briefings and training

- Include components around diversity and inclusion, especially as part of codes of conduct, in the induction process, and explore how these link with personal responsibilities for security and organisational duty of care.
- Consider the degree to which pre-departure training and briefings address diverse profiles.
- Do not 'target' individual people in inductions and pre-departure briefings; instead, keep these generic, to be received by all staff, and provide specific guidance and signposting that address diverse personal profiles.
- Include examples in the security training from practice that relate to different ethnicities, people with disabilities and different genders/sexualities, as well as issues related to intersectionality.
- Ensure that trainers have the necessary skills, information and training to deliver sessions that are suitable for staff with a diversity of profiles.
- Formally train security focal points on diversity, equality, inclusion, anti-discrimination and how these interact with duty of care obligations.
- Clarify during security-related training that all individuals, no matter what their personal profile is, will be vulnerable to threats in given circumstances. It is important to not fall into the trap of assigning vulnerability to specific groups, e.g. women, LGBTQI staff, etc.

KEY RECOMMENDATIONS

Deployment

- Take all reasonable steps to keep staff safe and secure.
- Keep deployment decisions transparent and in line with security risk management and human resource policies and procedures. Involve dialogue and discussion with the aid worker(s) concerned where appropriate.
- Ensure that staff with minority profiles have the confidence to work with security focal points to ensure deployment security measures reflect the concerns of particular profiles.
- Consider asking detailed questions to ensure the suitability of accommodation, particularly for staff with minority profiles. Some examples would be:
  - Is it accessible to people with disabilities?
  - How could it be made accessible to people with disabilities?
  - How accessible is it for staff to get to and from key locations (e.g. the office and amenities)?
  - Are there spaces where staff can hold private conversations/phone calls?
  - Can bedrooms and wash facilities be securely locked?
- Ask about the potential for reasonable changes to be made to deployment plans or whether alternative options can be found before deciding that the posting is not appropriate for a particular profile.
- Ensure that aid workers' experiences post-deployment inform pre-deployment trainings and briefings.

KEY RECOMMENDATIONS

Travel

- Consider the differing security risks faced by travellers on short visits in comparison with those on longer-term deployments when looking at mitigating measures.
- Encourage an open culture within senior management and security focal points, to give staff with minority profiles the confidence to come forward and help ensure travel management decisions reflect the concerns of particular profiles.
- Ensure in-country travel checklists include questions about how different profiles will be kept safe from both internal and external threats.
- Remind all travellers of the incident reporting mechanisms available to them, as well as the consequences of harassment.

KEY RECOMMENDATIONS

Incident management

- Induct all on the use of incident reporting procedures, including what happens after an incident gets reported and how confidentiality is maintained.
- Raise awareness of when an incident may be related to the staff member's personal profile.
- Train several members of staff to receive incident reports.
- Put in place a comprehensive data protection policy which is shared with all staff.
- Establish clear disciplinary procedures for staff who engage in hostile behaviour towards colleagues due to their personal profiles, raise awareness among staff of the consequences of such behaviour, and ensure disciplinary measures are implemented consistently.
- Develop an incident response checklist that considers diversity and incidents affecting staff with minority profiles.
- Develop an anonymous equality and diversity monitoring form that accompanies an incident report template and develop a process on how to make use of this information in a confidential manner.
- Ensure clarity between security focal points and HR staff on the responsibility of monitoring incidents between staff that may be motivated by personal profiles.
- Carry out a regular anonymous survey of staff to understand the scale and nature of security incidents, including harassment that has not previously been reported, and to identify underlying attitudes.

KEY RECOMMENDATIONS

Crisis management

- Crisis management teams should consider these key questions when planning for different staff profiles in a crisis:
  - Are any additional evacuation or relocation measures necessary for staff with disabilities (natural hazard/conflict-driven/medical)?
  - Are different crisis management approaches necessary when dealing with the abduction of a local staff member versus an international staff member? What about the additional risks associated with a particular profile?
  - What steps should be taken if an aid worker is arrested on suspicion of same-sex activity in a context where this is illegal?
- Think carefully about the diversity of staff available to conduct a post-crisis debriefing, and ensure these individuals are aware of the assumptions they may make about the profile of the person they are debriefing.
- Provide a list of recommended post-crisis support, e.g. psychosocial care, with a short description of particular providers' areas of expertise.
- Ensure that insurance policies consider the diverse needs of staff based on their personal profiles.
- Include information on insurance cover within induction programmes, so that if there are exclusions then staff are aware that they might need to have their own insurance policies in place.

KEY RECOMMENDATIONS

Data and information sharing

- Identify what data is already collected on different profiles in recruitment, deployment and operations, as well as incidents and crisis management.
- Identify the gaps in data being collected, and decide what is reasonable to collect at each stage to ensure the safety and security of staff.
- Review methods of data collection, including equality and diversity monitoring and incident reporting for a diverse range of staff profiles.
- Identify the staff best placed to collect data in recruitment, deployment and operations, as well as incidents and crisis management.
- Train staff in data collection, data protection and how to turn the data into useful information that will support security risk management processes.
- Communicate data protection policies to all staff and strictly abide by these guidelines.
- Pilot data collection methods, and seek feedback from aid workers with minority profiles.