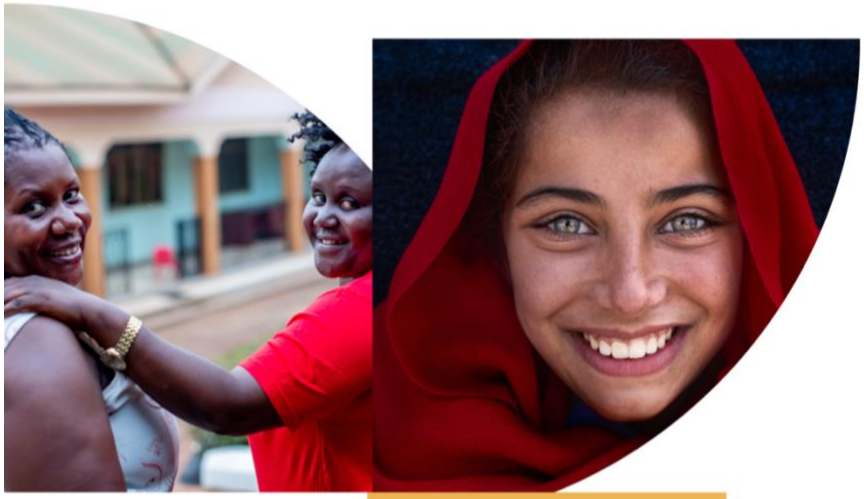
actionaid

2023



WWW.ACTIONAID.ORG

GLOBAL SAFETY & SECURITY POLICY

Table of Contents

1. Introduction

ActionAid's Strategy 2028 (Action for Global Justice) commits us to fight global poverty and injustice and shift power by working with people living in poverty and exclusion. Our mission requires a certain level of risk tolerance for us to remain purposeful and impactful. Whether it is driving social change, building resilience, or responding to a humanitarian crisis, our work involves an inherent and foreseeable exposure to safety and security risks which we cannot completely eliminate. However, the Duty of Care towards our personnel requires us to assess and mitigate serious risks (foreseeable or unforeseeable), build capacities to prevent and respond to security incidents and create a culture of empowered, informed, and calculated risk-taking.

The Global Safety & Security Policy presents the essential Security Risk Management (SRM) foundations and mechanisms per our legal and ethical commitment to our people. This document will be the basis and essential reference guide for all corresponding safety, security and health policies, procedures, and practices.

1.1. Key Terms

The key terms and abbreviations used throughout this document are given below. Policy users must read and understand them in order to understand the Policy.

- **Accompanied Legal Dependant (s):** This means accompanying Partner/Spouse and dependent children of a relocated or posted personnel.
- **ActionAid (AA):** where the word ActionAid or abbreviation AA is used, it refers to the entire ActionAid Federation.
- **ActionAid Entities:** This phrase refers to all legal entities of ActionAid, such as Members, Country Programmes, and GS.
- **ActionAid International (AAI):** This term includes the Global Secretariat, Country Programmes, and any other programme/project under AAI's legal and management responsibility.
- **ActionAid's People or Personnel:** These are inclusive terms which refer to all personnel to whom ActionAid's Security Policy applies, in part or whole. For the application of this Policy, the personnel categories are as follows:

  A/ *All staff categories, including full-time, part-time, paid, unpaid, national, international, interns, full-time consultants unless agreed otherwise (full application)*

  B/ *Volunteers and trustees when working under ActionAid's instruction (some sections apply)*

  C/ *Accompanied legal dependants (some sections apply)*

  D/ *Personnel legally under our duty of care, such as those visiting or working at our premises, those working or travelling under our instruction and security responsibility, and invited participants of ActionAid events, which could include rights-holders, community members and partners (some sections apply).*

- **Crisis:** Circumstances that constitute a severe threat to the organisation and pose extraordinary task demands requiring coordinated actions taken under conditions of uncertainty and time pressure. If not managed well, an incident or critical incident can become a crisis and affect the federation beyond the safety and security risks.
- **Critical Incident (CI):** Any situation or event that has caused severe physical, emotional, or mental harm to ActionAid personnel, such as sexual assault, abduction, arrest or detention, casualty, medical emergency, a threat to life or loss of life to a security event, or any other which the Incident Management Team considers to be a serious occurrence based on the context, the implications, or the available incident management capability.
- **Duty of Care (DoC):** Duty of care is ActionAid's legal and moral obligation to take all possible and practicable measures to reduce the risk of harm to our personnel. The DoC comprises four specific sub-duties (i) Duty of information, (ii) Duty of prevention, (iii) Duty of monitoring, and (iv) Duty of intervention.
- **GS:** Global Secretariat
- **Incident Management Team (IMT):** A high-level team designated and trained to deal with safety, security, health, and other incidents impacting our personnel.

The IMT must be headed by the senior-most manager or the Country Director, as the case may be. The IMT must have appropriate training, decision-making authority, and access to emergency budgets to ensure incident response and recovery, support for the affected personnel, and business continuity efforts. In many cases, the IMT will also be equipped to manage SHEA and Safeguarding incidents/concerns.

- **Incident:** Any situation or event that has caused physical, emotional, or mental harm to ActionAid personnel.
- **International Crisis Management Team (ICMT):** This is the highest level of incident/crisis management team headed by the Secretary-General or another ILT member appointed by the SG. The ICMT will be activated when an incident is escalated to Level 03 as outlined in the Incident and Crisis Management Protocol.
- **Near-Miss:** Incidents that have occurred in the area where ActionAid is working but have not directly affected our personnel; or any situation that has narrowly avoided becoming an incident.
- **Posted Staff:** These terms refer to anyone requested to reside and work at a location other than their usual place of residence for ActionAid's business, on ActionAid's request and under ActionAid's responsibility. Postings may be accompanied or unaccompanied, depending on the applicable HR criteria.
- **Safety and Security:** The terms safety and security are used interchangeably in this document, and wherever 'security' is used, it means to include 'safety' and vice versa. However, technically correct definitions are as follows:
    - ***Safety:*** *Freedom from risk or harm resulting from* ***unintentional or accidental acts****, events, or hazards.*
    - ***Security:*** *Freedom from risk or harm resulting from* ***intentional acts of violence, aggression and/or criminal acts*** *against personnel, programmes, or assets.)*
- **Security Evacuation:** The physical movement of personnel across an international border to reduce exposure to heightened /intolerable risk. The evac process may involve hibernation (bunkering down) and relocation (movement within the national borders).
- **Security Relocation:** The physical movement of personnel within the country to reduce their exposure to heightened /intolerable risk. The process may involve hibernation (bunkering down).
- **Senior Management:** This term refers to the Senior-Most Manager and Senior Leadership Team combined.
- **Senior-Most Manager:** This term refers to the highest management position at the Country and Global Secretariat. At the Global Secretariat, it refers to the Secretary-General, while at the country level, it refers to the Country or Executive Director (or another role of similar seniority).
- **SHEA & Safeguarding:** Sexual Harassment, Exploitation and Abuse, Child Abuse, and Adult at Risk Abuse
- **SRM:** Security Risk Management, where security includes safety.

1.2. Policy Statement and SRM Framework

ActionAid is committed to creating a culture of effective safety & security risk management (SRM) which meets our DUTY OF CARE responsibilities to our people. ActionAid seeks to create this culture by investing in the development of capacities and systems that enable us to minimise safety & security risks while maximising the impact of our work, by establishing reasonable and practicable measures to mitigate and respond to adverse events, and by empowering our personnel to take responsible and informed security decisions.

ActionAid's Safety & Security Risk Management (SRM) Framework explains the architecture, roles, responsibilities, and arrangements we will put in place to support our Policy statement. The diagram below illustrates the essential building blocks of our SRM Framework and how they fit together.

1.3. Scope & Applicability

The Global Safety & Security Policy (also known as the 'Security Policy' or the 'Policy') focuses on the **Protection of ActionAid's People** (see definition in 1.1). Some sections also apply to other organisational assets such as **programmes, property, processes, and premises** with the primary aim of protecting the people.

This is one of the core organisational policies, and its full and effective implementation is binding upon all ActionAid entities. The Security Standards are fully adaptable, and their implementation will be subject to their usefulness and applicability in each context.

The Security Policy must be read, understood, and implemented in conjunction with other organisational policies, especially **SHEA and Safeguarding, HR Policies, Employee Code of Conduct, Information Security, Whistleblowing, Assurance, Policy on Principles and Approaches for the Protection of Lives and Livelihoods of Affected Communities in Emergencies,** and **Humanitarian Preparedness and Response Handbook.**

The Policy does not apply to partner organisations or communities[1] we serve (see Standard 13- Support for Partner Organisations.).

In situations where local or national laws contradict this Policy, ActionAid entities must follow these laws if they are more robust regarding the employer's duty of care obligations.

1.4. Accountability and Responsibility

At an individual level, all **ActionAid Personnel** will be responsible for their personal safety and security and accountable for their decisions. Personnel will actively promote a culture of calculated risk-taking and effective SRM across the federation. They will respect other colleagues' risk threshold and not engage in 'mission bullying'[2]. At the same time, they will report reckless behaviour and actions that pose unnecessary and excessive risks to other personnel and the organisation. Personnel are also expected to refrain from any action or activity that jeopardise their own or others' security, which includes aspects of digital safety, online behaviour and the use of electronic and social media.

Institutionally, the **Boards of Trustees** will be the safety and security risk owners, holding the **highest-level accountability** for approving, financing, implementing, and ensuring compliance with this Policy across their governance remits (International Board for ActionAid International (AAI) which includes the Global Secretariat and Country Programmes, and National Boards for their respective ActionAid Member - Associates and Affiliates).

The **Senior-Most Managers** (AAI Secretary General, Country/Executive Directors, or a position of similar seniority) will hold the **highest-level responsibility** for contextualising, financing, implementing, and ensuring compliance with this Policy across their management remits. They will fulfil this responsibility by working closely with the **Senior Leadership Teams** (International and Global Leadership Teams and Country Management Teams).

The **Global Safety & Security Lead** will provide technical advice and strategic direction on the SRM framework, including Safety and security principles, standards, and operational guidelines.

The operational security management will be shared across different levels in the Federation as follows:

Security Focal Points: Formally appointed SFPs with clear job expectations will provide technical and operational support for the Policy implementation. SFPs will

[1] Our community engagement is guided by "Global Policy on Principles and Approaches for the Protection of Lives and Livelihoods of Affected Communities in Emergencies" owned by the International Humanitarian and Resilience Team (IHART).

[2] A mission bully portrays those who want to follow security policies, or who are uncomfortable with the risks being taken, as 'too weak for this sort of work' and 'not experienced enough in dangerous environments' (Safer Edge)

be responsible for the safety and security tasks assigned to them, while the final security responsibility will continue to rest with the senior management.

- All ActionAid entities (Members, CPs), GS hub offices, and specific GS units with considerable operational security demands will appoint suitable full-time or part-time SFPs or security consultants.
- In the absence of a formally appointed Security Focal Person, the relevant senior-most manager will be the de facto SFP.
- The SFPs (Countries and GS) will be part of the global SFP team with functional accountability to the Global Safety Security Lead. Each formally appointed SFP will adhere to the Global SFP Team Charter and attend training and induction organised by the Global Safety & Security Lead.
- The SFPs will have a nominated deputy during periods of absence.

Human Resources and Operations Managers will ensure that familiarisation and compliance with this Policy are integrated into personnel hiring, onboarding, and performance management processes and clearly stated in the consultancy or service level agreements with suppliers and contractors. They will also ensure that ActionAid's HR and operations policies are aligned with the Security Policy.

Line Managers will lead by example and encourage, facilitate, finance, and enforce Policy compliance across their management remit. They will never condone, encourage, or approve any task or activity that contradicts our security risk management principles, which promotes reckless risk-taking or condones a disregard for the federation's security approach.

1.5. Compliance & Review

ActionAid will conduct annual compliance assessments using the Federation's assurance processes to assess the level of Policy compliance and identify gaps before they lead to severe risks. Any gaps thus identified will be addressed using organisational mechanisms described in the Global Assurance Policy. Our compliance approach will be empathetic and people-centred instead of being rigid or excessively mechanised. We will focus on listening, adapting and influencing actions and behaviours through a culture of calculated risk-taking and responsible security decision-making.

The Global Safety and Security Lead will conduct a consultative Policy review every five years or earlier in case of a strategic shift or a major restructuring to ensure its relevance and applicability across the Federation.

2.Safety & Security Principles

ActionAid's SRM (Safety & Security Risk Management) approach is underpinned by the following **Safety & Security Principles,** which will be **consistently applied** across the Federation.

2.1. Primacy of life

As far as possible, ActionAid will prioritise the safety and security of its personnel over property (assets), reputation, and programme continuation. We will never demand or allow our people to endanger their lives to protect material assets or another person, safeguard organisational reputation or meet a programme deadline. While we will always use ActionAid's financial resources responsibly, we will not compromise personnel's safety, security, and mental and emotional wellbeing to save costs.

2.2. Acceptance of our Work

We will seek acceptance of our work as the primary strategy for reducing safety and security risks to our people. This means nurturing and maintaining strong working relationships with local actors through networking, relationship-building, proactive communication, transparency and accountability, respectful personal conduct, and values-driven programming.

2.3. Dynamic Risk Appetite

ActionAid's appetite to accept safety and security risks will not be a single, fixed concept. We may take greater risks to fulfil a critical programme need if appropriate risk control measures have been put in place. The extent of risks that ActionAid will tolerate will be limited by our ability to manage those risks. This means that the senior management will objectively analyse any situation that exposes ActionAid to severe or new risks before deciding to proceed. Refer to Programme Criticality & Security Risk Guide

2.4. Proactive & Systems Oriented

Prevention and proactive risk management are the fundamental principles of ActionAid's Security Risk Management approach. ActionAid will actively strive to prevent incidents instead of relying on the response mechanisms alone. To ensure proactive risk management and preparedness, we will never adopt an ad hoc approach towards SRM. Instead, we will invest in systematising and embedding safety and security risk management into key programmatic and organisational processes and make continued investments in training and capacity enhancement of our personnel.

2.5. Context-Specific

SRM will not be treated as a ''box-ticking'' exercise but will always be informed by the local context and people's lived experiences, as far as practicable. We will empower our people to think creatively and adapt to the diverse factors influencing their exposure to safety and security risks.

2.6. Holistic & Integrated

SRM will not be an isolated process but integrated into the Federation's holistic risk management approach. All significant organisational risks will be managed through appropriate policies and mechanisms, including safety and security, SHEA and safeguarding, financial, legal, information, cyber, reputation and others.

2.7. Equitable & Inclusive

ActionAid recognises that our people face varying types and degrees of safety and security risks due to their gender, ethnicity, neurodiversity, nationality, religious affiliation, health, race, sexual orientation, physical and mental ability, and other personal characteristics. As

such, people may require exceptional support beyond organisational policies to perform their duties safely. We will endeavour to listen, learn, and make our safety and security policies/practices as inclusive and equitable as possible.

2.8. No Ransom

If ActionAid personnel are taken hostage or kidnapped while on official business, ActionAid will do everything in its power to facilitate their safe and unconditional release. However, we will not negotiate, transport, or pay a ransom, nor concede to any other extortion and criminal demand, as this will only increase the risk for our people.

2.9. No Firearms

ActionAid personnel will not carry firearms and other lethal weapons while on ActionAid business, on ActionAid premises or on board any vehicle owned, hired, or rented by ActionAid. Where armed protection is assessed to be essential for safety and security or programme continuity, all ActionAid entities will adhere to ActionAid's protocol for armed protection.

2.10. Right to Refuse & No Right to Remain

Personnel working with ActionAid will have the right to refuse or request a withdrawal from an assignment (including travel) under the following circumstances:

- **Lack of information:** Personnel have not received satisfactory information about the risks and organisational risk management measures. If this information has not been made available despite requests, the right to refuse will apply.
- **Inadequate security support:** When the organisational risk management measures fall short of the standards prescribed in this Policy or what is considered reasonable in the local context.
- **Personal factors:** When individual risk factors outweigh the available safety and security support. (Also read 2.1.primacy of life)

As far as possible, the request to refuse or withdraw from an assignment will be respected by ActionAid without any negative consequences - unless it puts anyone else at risk or repeatedly impacts the requester's ability to perform their contractual responsibilities. Such situations will be resolved by the Line Management in consultation with the relevant HR.

ActionAid will always retain the right to suspend activities, cancel or postpone travel, or withdraw personnel from assignments or locations depending on the risk environment and the organisation's risk management capacities. **ActionAid's decision will be binding on all personnel. Refusal to comply will be treated as insubordination resulting in disciplinary measures per the applicable HR policies.** Relocation and evacuation orders will only apply to the posted, deployed or travelling personnel where their safe return to the point of origin is ActionAid's legal and ethical duty. See Standard 04: Security Hibernation, Relocation and Evacuation

3.Safety & Security Standards

The following **Safety & Security Standards** have been developed to support effective risk management across most contexts where ActionAid works. These standards will be contextualised, financed, and implemented by the senior-most managers and senior leadership teams under the ultimate accountability of the relevant Boards of Trustees. **This**

is the only section of the Security Policy that can be modified as best suited to the ground realities. Any variation or omissions must be authorised by the relevant risk owners and those holding the highest security responsibility (Boards, Senior Management). Given the diversity of ActionAid programmes and locations where we work, ActionAid entities will be individually responsible for planning and implementing additional measures relevant to their political, legal, security, climatic and programmatic contexts. Different units or teams within an ActionAid entity may also implement additional or specific safety, security and health measures for their teams depending on their risk exposure.

Standard 01: Security Focal Point (SFP)

a) As outlined in the 'Accountability & Responsibility' section, each ActionAid entity which means Affiliates, Associates, Country Programmes, GS offices, as well as specific GS units with considerable operational security demands, will formally appoint suitable Security Focal Person(s) with clear job expectations parameters of authority, and budgets.

b) SFPs will be responsible for the safety and security tasks assigned to them via a formal job description and annual performance dialogue. The overall SRM responsibility will continue to rest with the senior management.

c) In the absence of a formally appointed Security Focal Person, the senior-most manager will be the de facto SFP.

d) The SFP will have a nominated deputy for the period of absence.

e) The SFPs (Countries and GS) will be part of the global SFP team with functional accountability to the Global Safety Security Lead. Each formally appointed SFP will adhere to the Global SFP Team Charter and attend training and induction organised or recommended by the Global Safety & Security Lead.

Standard 02: Programme Risk Assessment (PRA)

a) All ongoing and future programmes, projects and campaigns will be risk-assessed using ActionAid's PRA procedure, and each risk will be managed using appropriate risk management actions.

b) Each risk management action will be budgeted, assigned a suitable timeframe and a designated task manager.

c) For specific programmatic activities, additional risk assessments will be carried out if the anticipated risks have not been adequately addressed in the standard PRA. LRP Activity Risk Assessment and Research Risk Assessment

d) All programme risk assessments will be updated at least once every 12 months, and any PRA older than 12 months will be invalid. In fluid and volatile contexts, the PRA may need more frequent revisions, which the senior management will ensure in consultation with the SFP.

Standard 03: Contingency Planning

a) In case of an anticipated high-threat event (trigger event), which could be political, social, security, environmental or climate-related, the concerned ActionAid entity or office will proactively devise and implement a comprehensive scenario and preparedness plan, also known as a Trigger event preparedness & contingency plan for the safety and security of ActionAid Personnel. This plan differs from the programme-focused Emergency Preparedness Plan and Response/Recovery Strategy.

b) If necessary, the plan will include programme suspension or scale-down indicators to protect ActionAid Personnel from imminent harm proactively.

c) Each risk management and mitigation measure will be assigned appropriate budgets, timeframes, and task owners.

d) The plan will be updated as frequently as needed, and new task managers will be assigned in case of absence or turnover.

Standard 04: Security Hibernation, Relocation and Evacuation

a) In volatile contexts, appropriate security hibernation, relocation and evacuation plans will be developed through a consultative and inclusive process.

b) The hibernation, relocation and evacuation plans will be periodically updated and tested with all concerned personnel so that roles, responsibilities, and operational modalities are clearly understood before a real-life situation occurs.

c) Medical evacuation (medevac) will be included in the possible scenarios and periodically tested.

Standard 05: Travel & Postings

a) Personnel travelling for ActionAid business (categories A, B, C) and the travel approvers will ensure full compliance with the applicable Travel Safety Procedures relevant to the type of trip (domestic, international, humanitarian).

b) ActionAid travellers will always have the right to refuse a business trip subject to the conditions in Principle 10: 'Right to Refuse'.

c) All business trips will be covered by suitable travel and personal accident insurance provided by ActionAid.

d) For travel safety risks per destination/country, ActionAid will use a standard reference in order to ensure consistency across the Federation. However, all business trips will generally be treated with similar caution regardless of the destination's risk level.

e) All business travellers (categories A, B, and C) will receive a suitable travel security training organised and paid for by ActionAid. Personnel will be required to repeat the training every two years or before the expiry of their completion certificate.

f) When travelling to another ActionAid entity, travellers will receive a context-specific pre-travel risk briefing organised by the host, which will address the individual risk factors, activity risk factors and contextual risks.

g) When travelling to a country where ActionAid does not have a presence or while attending an external meeting/event, the travellers may request a professional risk briefing delivered by a suitable third party.

h) Posted personnel and accompanied legal dependants will receive appropriate safety and security support, including vaccines/prophylaxes, location-specific security briefing, security training (adults only), support for safe accommodation, wellbeing support (including psychosocial and mental health), medical insurance and any other location-specific support for the duration of the posting.

i) Personnel will receive appropriate safety and security support depending on their individual circumstances (race, nationality, ethnicity, gender/gender identity, sexual orientation, disability, other) as these factors may expose people to specific risks. See Principle 7, Equitable and Inclusive

j) The senior leadership and board members will avoid routinely travelling together to prevent a situation where an accident or emergency affects the entire leadership or governance team. The only exception is when the risk has been

weighed against the benefits and a contingency response mechanism has been put in place.

k) To support work-life balance and enable ActionAid to provide support in case of an incident, personnel will try to travel within office hours and on a working day. If this is not possible, every effort will be made to arrive at the destination during daylight hours on a working day.

l) Travel risk management will include all forms and modes of business travel, such as:

Surface Travel

- Only authorised and trained drivers with valid driver's licenses who are familiar with the local driving conditions and rules will drive an ActionAid-owned or rented vehicle. Such authorisation is best granted by the senior manager closest to the ground unless the relevant ActionAid entity has another authorisation procedure in place.
- If relevant to the context, based on a programme risk assessment, it is the responsibility of the senior management closest to the ground to ensure a system of authorised designated drivers available 24/7 for emergencies, including security relocations or medical evacuation (where ambulances may not be available).
- Intoxicated personnel or those on medications that cause drowsiness, anyone suffering from visible stress, lack of focus, sleep deprivation or feeling physically or mentally unwell will not drive a motor vehicle for ActionAid. Such personnel must turn down any request to drive for ActionAid using this policy provision.
- ActionAid will always use safety-checked motor vehicles that meet our essential safety and security standards. Vehicle Safety Checklist.
- All drivers and passengers will wear seatbelts throughout the journey.
- Those driving or travelling by motorbikes (all types) will always wear a helmet and any other safety equipment considered necessary and appropriate in the local context.
- Those driving for ActionAid must always follow the local laws, including speed limits, registration requirements and any other legally binding rules applicable in the local context.
- Those driving an ActionAid vehicle/bike will not use mobile phones or participate in virtual meetings unless they can safely park the vehicle/bike for the call. This also applies to persons driving their private vehicles/bikes. This rule can only be bent when there is a serious safety and security threat, and the driver must make or receive a phone call to avert an imminent danger.

Air Travel

- ActionAid will only use reputable travel agents to book flights and will brief them on ActionAid's safety and security expectations as part of our service level agreement.
- Personnel will be entitled to choose more expensive options (where available) where flight departure/arrival time and layover duration are unsafe or excessively inconvenient for the traveller.

Other Modes

- Only safe and reliable boats and ferries will be used for ActionAid business, and all travellers will have access to life vests and other necessary safety equipment.
- If personnel are requested to use public transport for official work, including taxis, trains, trams, buses or motorbikes (all types), bicycles, buses, or by foot, the relevant management will assess the safety of such options and will provide appropriate support to all personnel.
- As much as possible, the management will provide the safest travel mode for official trips, which generally excludes the usual commute to and from the workplace.

Personnel using personal transport and accommodation

- Personnel are discouraged from using personal vehicles for official engagements unless authorised by the senior-most manager.
- Personnel will avoid making personal accommodation arrangements while travelling for ActionAid unless approved by the senior-most manager.

Standard 06: Premises Security

a) Office spaces and other premises will be hired, leased, or used only after conducting a premises risk assessment.

b) All items of value will be covered by appropriate asset insurance.

c) All IT equipment and data will be protected with passwords and cloud backup in accordance with the applicable IT policies.

d) All accommodation facilities used by ActionAid, such as hotels, guest houses, bed & breakfasts, or hostels, will be safety-checked using ActionAid's accommodation safety checklist.

Standard 07: Armed Protection

a) All ActionAid entities will adhere to ActionAid's protocol for armed protection in locations where armed protection is essential for personnel safety or programme continuity.

Standard 08: Meetings and Events

a) All ActionAid events and meetings will be organised per the ActionAid's safety and security guidelines for meetings and events.

b) The organisers and approvers of large meetings will be responsible for ensuring appropriate safety and security arrangements for their event, as laid out in the above guideline.

Standard 09: Safe and Reliable Communication

a) While travelling or being posted for ActionAid's business, the personnel in categories A, B, and C will have safe and reliable communication capabilities such as mobile phones and airtime/data/internet to report security incidents and receive support.

b) In case of unstable or unreliable mobile coverage or frequent outages, VHF/HF radios, satellite phones, and internet connections will also be provided.

c) In programme contexts assessed to be high-risk and volatile according to a valid programme risk assessment (PRA), including contexts prone to environmental and climate-related hazards, a headcount procedure will be implemented and regularly tested to ensure its effectiveness and reliability. Such contexts may also require an established and tested protocol for complete communication breakdown.

Standard 10: Reporting Security Incidents and Concerns

a) ActionAid Personnel will report all safety & security incidents or near misses they experience while performing ActionAid duties or while under ActionAid's responsibility.

b) A straightforward and easy-to-follow incident reporting procedure will be put in place and communicated to ActionAid personnel. (Incident and crisis management protocol)

c) Each ActionAid country and GS Hub will have a designated and trained Incident Management Team (IMT) whose members will act as the first point of contact in case of a security incident involving ActionAid personnel. Larger teams may decide to have multiple IMTs to cover specific geographical locations, and if practically viable, the senior management team may double as the IMT.

d) The IMT will be chaired by the senior-most manager available closest to the ground, with ultimate responsibility resting with the senior management (Country or GS Hub).

e) The IMT will have appropriate training, decision-making authority and access to emergency budgets to ensure incident response and recovery, support to the affected personnel, and business continuity. In many cases, the IMT will also be equipped to manage SHEA and Safeguarding incidents/concerns.

f) In addition to the security incidents, ActionAid personnel will report all security concerns and grievances, including policy noncompliance, repeated or deliberate security breaches, and lack of support, as outlined in ActionAid's Commitment to Personnel. Such reports will be made to the relevant senior management in the first instance. If travelling, the concern will be reported to the host and own line management. Most concerns will be addressed at this stage in a respectful, consultative, and inclusive manner. Otherwise, the concerned individual may escalate the matter using ActionAid's Whistleblowing Mechanism.

Standard 11: Incident & Crisis Management

a) The Global Secretariat will have an International Crisis Management Team (ICMT) chaired by the Secretary-General (SG) or another member of the International Leadership Team (ILT) appointed by the SG.

b) In case of an incident, the IMT and ICMT will follow ActionAid's Incident and Crisis Management Protocol which comprises three escalation levels. **[Level 01]** The IMT

manages the incident without requiring support from the Global Security Lead. **[Level 02]** The IMT manages the incident with the active support and involvement of the Global Security Lead and any other functional or management expertise. Most incidents in ActionAid will be managed at Levels 01 or Level 02. **[Level 03]** The incident is very serious, and the ICMT is activated, led by ActionAid International's Secretary General or another ILT member designated by the SG.

c) The IMT and ICMT must ensure proper incident documentation and maintain a record of actions and decisions taken. All incidents must be followed by a written Incident Report produced by the concerned IMT within two (02) weeks of the incident resolution. Download Incident Report Template

d) Each ActionAid entity will conduct an annual analysis of all incidents/crises reported during the year to identify trends and efficacy of the remedial actions taken and to decide and implement further actions as necessary. This trend analysis will also inform the allocation of emergency funds for the following year.

Standard 12: Networking

a) Networking with security and non-security stakeholders will be central to our acceptance strategy and effective programming. ActionAid will seek to develop and deepen our relationship with key external stakeholders across our areas of operation following a comprehensive stakeholder mapping exercise.

b) ActionAid entities will participate in external humanitarian, human rights and development networks, communities of practice and formal and informal coordination mechanisms to exchange useful SRM knowledge and alerts. Where these networking opportunities do not exist, ActionAid will explore possibilities to initiate such conversations and lead on inclusive and dynamic SRM practices.

Standard 13: Support for Partner Organisations

Our security policies do not apply to partners other than the sections applicable to category D personnel. Nonetheless, our duty of care and inclusive SRM approach require that we proactively collaborate with our local and national partners in all aspects of SRM, such as:

a) Joint SRM processes and active collaboration on safety and security.

b) Training, induction, and financial support to enhance the partners' SRM capabilities where reasonable and practicable.

c) Proactive dissemination of security information and resources, including policies, templates, and guidelines, while creating opportunities to learn from the partners' experience and local knowledge.

d) Technical guidance and support for incident handling and response (including psychosocial and mental health support).

e) Inclusion and representation in security networks and security-focused communities of practice.

Standard 14: Health & Wellbeing Support

HR policies will include necessary standards and guidance on issues related to personnel' s wellbeing, including mental health. Where HR policies fail to address these critical areas, the relevant senior management will be responsible for updating the policies and aligning them with the federation's security framework.

a) Appropriate risk insurance such as life, Medical /health insurance (Personnel categories A, C)

b) Work-life balance, flexible work modalities and mandatory leave (Personnel categories A, B)

c) Confidential psychosocial and mental health support (All personnel categories)

d) Support for personnel with caring responsibilities, for those facing challenging personal circumstances and for those with special needs (All personnel categories)

e) Health and safety equipment, including personal protective equipment, Post-Exposure Prophylaxes (PEP), and first aid kits. The information about safety equipment (including PEP kits) will be relayed to the concerned personnel with a clear procedure for accessing and using this equipment. Depending on the context, the management may need to consult the SHEA and Safeguarding and HR focal points to develop workable and context-specific SoPs (All personnel categories).

f) Risk-assessed accommodation and equitable security provisions (all personnel categories).

g) Any other health and wellbeing support applicable to the local context, such as supplementary childcare, access to exercise facilities for deployed and posted personnel, travel accompaniment due to safety or cultural reasons, flexible timings, safe transport for official business, segregated workspaces, or any other (all personnel categories)

Standard 15: Security Induction & Training

a) ActionAid personnel (categories A and C) will receive appropriate personal security training corresponding to the context in which they are expected to work, travel, or reside. In contexts with a high threat of kidnapping, violent crimes, or environmental or climate-induced hazards, the training will include relevant modules and, where possible, practical simulations customised to the local context. Security Training Information

b) ActionAid personnel (categories A and C) will receive fire safety and first aid training with periodic refreshers per local regulations and travel needs. ActionAid travellers must be able to use a first aid kit even if the local laws do not require such training (Personnel categories A, B, and C).

c) Personnel hired on a longer term for driving ActionAid vehicles will be trained in defensive driving. This requirement may be waived for short-term hiring (less than three months) depending on the context and practicability.

Standard 16: SRM for Humanitarian Operations

a) In addition to the essential standards outlined in this Policy, specific humanitarian contexts may require additional or more robust SRM measures, without which our personnel will be exposed to a higher level of risk than we are willing to tolerate. In such contexts, the International Humanitarian and Resilience Team (IHART) will demand and enforce additional safety, security, wellbeing, and health measures binding on the relevant ActionAid personnel.

b) These requirements and measures will be communicated to the concerned personnel through the IHART communication channels and supported by the appointed Security Focal Point.

Standard 17: Security Budget

a) All ActionAid entities will set aside reasonable and adequate budgets to implement this Policy and ensure support to all personnel categories as outlined in this document. All project and programme proposals will include a budget line for security based on an informed analysis of the context and anticipated risks. Safety and Security Annual Budget Checklist

b) Security Focal Points will be consulted during the annual planning and budgeting exercise to ensure necessary security expenses are taken on board.

c) All ActionAid entities will set aside incident response budgets based on the annual monitoring and analysis of security incidents and the support required by the affected personnel.

Standard 18: Risk Insurance

a) As stipulated in this policy, ActionAid entities will ensure that suitable, appropriate, and adequate risk insurances are in place for people, property, premises, and programmes. It will be up to each ActionAid entity to assess their specific insurance needs and have appropriate covers in place.

b) Insurance covers, unless confidential, will be effectively communicated to the insured persons with periodic reminders.

c) Insurance policies will be regularly renewed, and any change will be communicated to the concerned personnel.

Standard 19: Written Security Plans

a) Each ActionAid entity, including the GS hub offices, will have written security rules and procedures (also known as a security plan), which will be communicated to all persons to whom they apply.

b) The security plan will be shared with partner organisations for a unified and consistent SRM approach across our programmes and projects.

c) The security plan will be developed, reviewed, and implemented in a participatory and inclusive manner, in consultation with personnel with diverse profiles, varied lived experiences, and roles.

d) The security rules and procedures enclosed in the security plan will be reasonable, practicable and relevant to the context in which they are applied.

e) To ensure the relevance and effectiveness of the security rules and procedures, ActionAid entities will conduct periodic security reviews and revisions of their local security plans. Any security plan older than 12 months will be considered invalid.

Standard 20: Compliance Monitoring

a) ActionAid entities will participate in the annual assurance process to gauge compliance with the Security Policy. Issues of noncompliance and partial compliance will be addressed on priority by the relevant management.

b) HR will ensure familiarisation and compliance with this Policy are integrated into personnel onboarding and performance management processes.

4. ActionAid's Commitment

As an ActionAid personnel, you are entitled to the following safety and security support while working under ActionAid's instruction or on its behalf. The list is not exhaustive, and additional support may be provided as necessary or legally binding. You must actively support the Federation to cultivate a strong Security Risk Management (SRM) culture. You should use this list to assess whether ActionAid is fulfilling its Duty of Care towards you, to make helpful recommendations, and, where necessary, to use your 'right to refuse' (Principle 10).

As far as reasonable and practicable:

1. ActionAid will prioritise your safety and security over programmes, reputation and property and not expect you to endanger your life to protect its reputation, material assets or another person.
2. ActionAid will empathetically consider your safety and security requests (beyond this policy) on a case-by-case basis.
3. Where ActionAid falls short of its security commitments, it will replan and rethink the assignment rather than expose you to foreseeable risks. You will have the right to refuse a task which exposes you to untreated and intolerable risks.
4. ActionAid will provide accurate safety and security risk information and be forthright about its safety and security risk management systems, structures, and capability. It will be honest and transparent and never mislead you into a false sense of security.
5. When you travel under ActionAid's responsibility and on ActionAid's request, you and your accompanied legal dependants will receive a location-specific risk briefing, security training (adults only), safe transport, safe accommodation, adequate means of communication (phone/internet/radio/Sat phone) to communicate and report security incidents, travel /medical insurance (or an effective alternative where insurance is not available), and security hibernation, relocation and evacuation support during your trip or posting when appropriate.
6. If you work from an ActionAid office, ActionAid will provide you with a safe, secure, and comfortable working environment and appropriate occupational safety training, including Fire Safety and First Aid.
7. ActionAid will establish a reliable incident reporting mechanism and provide you with the contact details /mechanism through which you can report incidents and concerns.
8. In case of a security incident, you and your next of kin/family will receive professional incident management support, including psychosocial support.
9. ActionAid will strive to harmonise and align all organisational policies that deal with ActionAid's people. Where there is a non-alignment of policies and provisions, ActionAid will choose the option most in favour of people's safety, security, and emotional, mental and physical wellbeing.

ENDS