MAG 24 01 Insurance Services – Relevant MAG Policies

This document contains copies of relevant MAG policies that inform and relate to MAG's insurance arrangements.

GLOBAL SECURITY POLICY (last approved March 2023)

1 - POLICY OBJECTIVE

MAG has a legal and moral duty of care to ensure, as far as is reasonably practicable, the safety and security of personnel working in and visiting its countries of operation. The security policy's objective is to enable MAG personnel to carry out their work globally, while minimising risks to staff and the organisation. The risks inherent in MAG's working environments may not be able to be eliminated but must be managed to within acceptable limits.

2 - SCOPE AND APPLICATION

This policy applies to MAG staff, consultants, interns, volunteers, board members, donors and other affiliated personnel during working hours and 24 hours a day when deployed away from their home residence on MAG business.

2.1. Partner Organisations:

When working with partner organisations MAG must be satisfied that they are ensuring duty of care for their own contracted personnel. The Partnership Agreement should explicitly define that the partner organisation is responsible for providing a safe and secure environment for its personnel and that they will take appropriate measures to do so, ensuring that security is managed effectively.

MAG will formally evaluate the partner's security management capacity by conducting due diligence prior to, or during the project start-up phase, identifying weaknesses and areas in which support may be offered to the partner, to develop their capacity and reduce risk. The 'Partner Organisation Security Due Diligence Guidance' document details MAG's approach.

MAG must take care to avoid extending duty of care, for example by stipulating exactly how the partner organisation is to manage its duty of care, by extending MAG insurance policies to cover partners, or by making specific comment on its policies and procedures. To do so creates a relationship of proximity and an implied duty of care.

2.2. Beneficiaries:

MAG is not responsible for the security of beneficiaries but will reasonably consider the security implications of its activities on them in risk assessments and project development. MAG's position with regards to safeguarding of beneficiaries can be found in the 'Safeguarding Policies'.

2.3. Non-Compliance:

Non-compliance with security policies, standards, procedures and/or guidance is a major risk to staff safety. Consequences of non-compliance will depend on the severity of the breach and may include a verbal or written warning, temporary suspension or termination of contract, progressed in line with the 'MAG Disciplinary Policy.' Country Directors (CD), Senior Managers in Country (SMiC), Regional Security Managers (RSM), Country Security Managers (CSM), Regional Directors (RD) and the Head of Global Security (HoGS) are all able to instigate an investigation and disciplinary process regarding potential breaches of security policies, standards, procedures and/or guidance.

2.4. Confidentiality:

The MAG Global Security Policy is an internal document, freely accessible to all MAG staff and associated personnel. It should be considered confidential and not distributed routinely outside the organisation unless agreed first through the HoGS.

3 - DUTY OF CARE

MAG's people are our most valued asset, more important than property, programming, or reputation. Through a partnership of management and staff, MAG shall strive to fulfil our duty of care.

3.1. Definition:

A duty of care is a legal obligation, imposed on an individual or organisation, to adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others. As well as a legal obligation, it is also the moral duty an organisation owes to its employees to protect them from

harm. MAG adheres to duty of care standards set in the British not-for-profit sector which are well-articulated and the most relevant to our activities.

3.2. To Whom Does MAG Owe a Duty of Care?

A duty of care is owed to all MAG staff, accompanying partners, consultants, interns, volunteers, board members, donors, project visitors and other affiliated personnel, during working hours and 24 hours a day when deployed away from their home residence on MAG business.

There may also be a duty of care for non-contracted personnel if there is a sufficient relationship of proximity (for example a non-contracted visitor undertaking a joint visit to a MAG project, or a partner organisation).

3.3. Fulfilling Duty of Care:

MAG fulfils its duty of care to its contracted personnel by:

- Assessing security related risks in all projects and countries of operation.
- Providing a robust global and country/ project-specific security framework to mitigate and manage these risks (including crisis management plans and country/ project security plans).
- Informing all staff and consultants of the threats they may face and threat mitigations through on-boarding, security training, pre-deployment security briefings and country workshops.
- Informing staff and consultants of their security obligations and responsibilities.
- Providing a mechanism for people to raise concerns about security.
- Providing travel health consultations, vaccinations, and prophylaxis for international travellers.
- Offering access to psychological support following traumatic incidents.
- Providing relevant insurance (including medical).
- Providing access to security related information and analysis.
- Obtaining the written informed consent of all personnel about the risks they may face.

4 - PRINCIPLES

4.1. Primacy of Life:

MAG values the life and health of its staff over program implementation and any physical assets. This principle should be at the centre of all security decision making.

4.2. Conflict Sensitivity:

MAG adopts a conflict sensitive, “do no harm” approach to programming, understanding that all interventions impact conflict dynamics as it is inevitable that these interventions will interact with the political, social and/or economic drivers of conflict.

MAG ensures that it understands the contexts in which operates, deliberately and systematically minimising the negative and maximising the positive consequences of our actions.

4.3. Humanitarian:

MAG is a humanitarian organisation. Underlining all our interventions are the principles of humanity, impartiality, neutrality, and independence which are rooted international humanitarian law.

All MAG staff must understand, consistently apply, adhere to and be able to articulate MAG’s work in respect to the humanitarian principles. When consistently applied - especially in situations of armed conflict and hostility - this enables MAG to distinguish itself from other actors, more safely access affected populations and contributes to reducing security risk to the organisation and partners.

- MAG’s mission is to save lives and build futures and accordingly humanity is the principal driver for any intervention, whether caused by conflict, violence or natural or man-made disaster.
- MAG distinguishes itself from other actors by acting with impartiality, responding based solely on need. Priority is given to the most urgent cases irrespective of race, nationality, gender, religious belief, political opinion, or class.
- MAG upholds the neutrality of intervention by refraining from taking sides in hostilities or engaging in political, racial, religious, or ideological controversies.
- MAG remains independent by being autonomous and is never subject to control or subordination by political, economic, military, or other non-humanitarian objectives.

4.4. Equity:

MAG will never provide a lower level of security provision to staff based on any protected characteristics. MAG may provide tailored guidance, advice and/or additional security provision to staff based on individual risk profiles and vulnerabilities.

4.5. Informed Consent:
Managing security will rarely reduce a risk to zero. Even with mitigations, MAG staff and consultants will still be exposed to residual risk because of uncontrollable external factors, particularly in high threat locations. In signing their contract, staff and consultants give their informed consent to such risk.

MAG will make every effort to actively share information with staff, visitors and consultants about any safety and security risks that they may face during their work and be open and transparent about where any capacity gaps in risk management provisions lie.

MAG commits to prepare its staff for this through security training, pre-deployment safety and security briefings, security on boarding, project/ country security management plans, provision of up-to-date information about the security situation in country, crisis and incident management plans and comprehensive travel, medical and other relevant insurance.

4.6. Right to Refuse or Withdraw:
Personnel have the right to decline a deployment or an activity without suffering disciplinary action if they think the risk to their security is unacceptable. This must be communicated in writing to their line manager, who will investigate with HR. Such requests will only be provided for where the evacuation does not expose the individual, or team to greater risk.

4.7. No Right to Remain:
Once a decision has been taken by MAG to withdraw from a specific area or to evacuate from a country, all international personnel must comply. No individual has the right to remain. In the event of evacuation, international personnel will be removed to their country of origin, or another safe location. Neither locally employed staff nor their dependents will be evacuated outside of their home country.

Authorisation to return to an area after withdrawal or relocation to a country after evacuation will be given by the Chief Executive (CE) on advice from the Director of Programmes (DoP). A security risk assessment must be completed before return.

4.8. Use of Armed Protection:
MAG do not use or hire armed personnel, either directly or indirectly, including UN force protection unless in exceptional circumstances. Arms and/ or armed personnel must never be allowed on MAG premises (including temporary ones), or in our vehicles, unless staff are threatened or coerced.

The use of armed protection will only be considered in exceptional circumstances, under strict criteria, assessed by the RSM and Head of Global Security and approved in writing by the CE. Any such request should adhere to 'Annex 1: Guidance on the use of Armed Protection' and be escalated by the SMiC, to their RD, to the DoP and finally the CE who must formally approve in writing any use of armed protection. This will be reviewed henceforth on a regular basis with the intention to cease the use of armed protection as soon as the risk level allows.

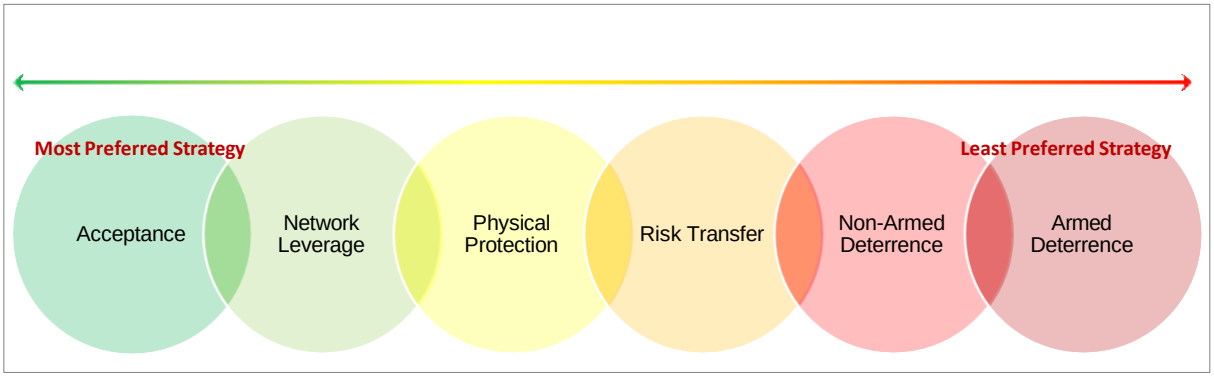
4.9. Weapons:
MAG staff will not carry or possess any weapons during their work at MAG expect when the handling and possession of weapons is part of the job requirement in line with the 'Policy on Personal Conduct'.

4.10. Rule of Law:
MAG staff must always comply with the national laws of the country in which they are working. Furthermore, MAG will not implement any measures or restrictions that contradict, undermine, or supersede any national or local laws that staff would otherwise be bound by.

5 - SECURITY STRATEGIES
5.1. MAG's Approach:
MAG seeks acceptance from the communities within which it operates by working through established governance and community structures in a participatory, culturally appropriate, and transparent way. Acceptance

is the preferred security strategy for MAG with a recognition that, as threats will not necessarily originate within a community but outside of it, additional protection measures and, in extreme circumstances, deterrence measures (e.g., the use of armed protection) will be required. SMiCs are responsible for implementing active acceptance strategies, following guidance from HQ. The strategy will consider and be adapted to suit the project/s and operating context.

5.2. Strategy Preference



Primary Security Strategy	
Acceptance	Reducing risk by gaining acceptance for our work from the communities in which we deliver operations
Complementary Security Strategies	
Network Leverage	Reducing risk, or responding to an incident by leveraging state and non-state allies to positively influence spoilers
Risk Transfer	Reducing risk through partner organisations, better placed to deliver aspects of our work safely (subject to due diligence and agreements)
Physical Protection	Reducing risk through physical protection measures
Non-Armed Deterrence	Reducing the risk or responding to an incident by containing the threat with a non-armed counter-threat (e.g., legal action)
Armed Deterrence	Reducing the risk or responding to an incident by containing the threat with an armed counter-threat. **In exceptional circumstances only and with the written permission of the CE**

6 - SECURITY CULTURE

MAG is committed to creating a strong and positive security culture in the following ways:

- Consultation and participation: staff across MAG are consulted in the development of safety and security policies and procedures.
- Strong security management framework: there are clear and understandable security policies and procedures that meet the needs of client groups; are commensurate with the risk; are followed by senior managers; are enforced.
- Buy in: the Leadership Team and Board of Trustees has buy-in to security policies and procedures and promotes adherence to these among staff.
- The security function: the security team enables, rather than dictates organisational objectives.
- Education: staff are educated through regular communication about security rules and the rationale behind these.
- Training: staff are provided with training to manage their own security and to learn appropriate security behaviours.
- Continual improvement: there is a process of ongoing feedback from users to test, review and adjust the security provision, learning from practical experiences and continually adjusting policies and procedures accordingly.

- Accountability: There are clear rules and consequences for non-compliance: people are more likely to demonstrate appropriate security behaviours if they know there is a consequence for non-adherence.

7 - ROLES & RESPONSIBILITIES

The CE has overall responsibility for the security of MAG staff, assets, programmes, and reputation. The day-to-day responsibility and decision-making authority for security is delegated to the DoP, RDs and CDs / SMiCs.

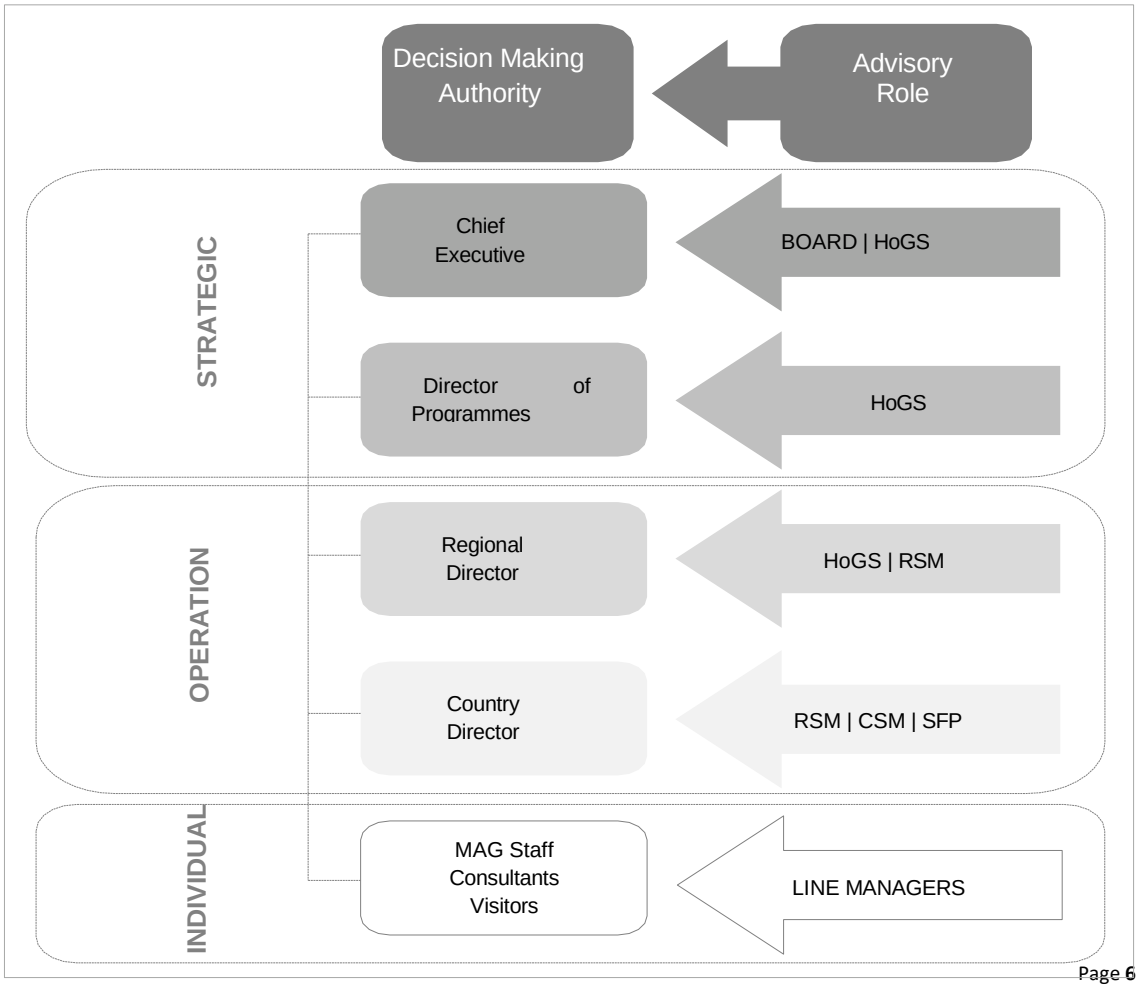
Security decision making at the programme level sits with the Country Director, not the Technical Operations Manager (TOM) or Technical Field Manager (TFM). This approach ensures the separation of security management decision making (and all related measures to reduce security risks) from operational management decisions, thereby avoiding a conflict of interest between security and operational delivery.

The HoGS, RSMs, CSMs and Security Focal Points (SFPs) provide security management and specialist advice, guidance and instruction to the decision-making authority at program, country, regional and global levels and assist in incident/ crisis management.

All staff with security management responsibilities will have these clearly articulated in their respective job descriptions, they are expected to fully understand what is required of them and will be appraised against this in their performance review.

To ensure the success of MAG's approach to managing safety and security risk, responsibilities for developing, implementing and maintaining them must be clearly defined and equally shared across all levels of the organisation: Strategic; Operational, and; Individual. If there is an absence of responsibilities being fulfilled at any one of these levels, then the safety and security of staff will ultimately diminish. These are further articulated down in '*Annex A: Roles and Responsibilities'*.

7.1. Security Decision Making Hierarchy:



7.2. Strategic Level:

At a strategic level MAG will:

- Ensure that there are processes in place to manage safety and security risks for personnel.
- Ensure staff and affiliated personnel are aware of their security responsibilities and adequately prepare them – through inductions, training, briefings, insurance, and medical coverage – to manage these.
- Ensure staff and affiliated personnel are informed of the context and specific risks inherent in their working environment and how these may be mitigated.
- Lead on the response and resolution of any major safety or security incident.

7.3. Operational Level:

Managers, Departmental Heads and Directors will implement MAG's approach to safety and security risk management by:

- Ensuring security minimum standards are implemented.
- Ensuring the consistent application of the humanitarian principles.
- Demonstrating good security behaviours and best practice.
- Prioritising and championing security.
- Reviewing security plans, policies, and control measures.
- Approving travel to programme locations and other visitations.
- Issuing advisories / directives in response to a major incident or emergency that has occurred in the same environment where MAG operates.
- Providing decision-making authority for temporarily suspending programmes, or withdrawing staff following an incident or deterioration in the security environment where MAG works.
- Assuming focal point duties for the verbal reporting of incidents and near-misses.
- Issuing staff with communications equipment or any other kit that is determined to be critical for staff security or safety.
- Delivering staff security inductions and / or country briefings.
- Forming official and unofficial networks for obtaining security information / intelligence.

7.4. Individual Level:

All staff at all times are responsible for:

- Adhering to the 'Policy on Personal Conduct'.
- Not behaving in a way that exposes colleagues, partners, or communities to any unnecessary risk.
- Adhering to security policies, plans, procedures, guidance, and advice.
- Attending mandatory security training.
- Complying with national or local laws that apply in locations where MAG operates.
- Being able to clearly communicate MAG's mandate.
- Ensuring the consistent application of the humanitarian principles.
- Respecting cultural or religious sensitivities that apply in locations where MAG operates or that are held by those who MAG seeks to support or work alongside.
- Treating MAG resources, information, equipment, and money responsibly, and report any cases of their misuse.
- Reporting safety and security incidents, near misses or concerns that have caused, or have the potential to cause harm to themselves, colleagues, partners, or communities.
- Not accepting bribes.
- Not using bribes, concessions, or extorting others to gain access to locations or sensitive information, or to coerce others to undertake work on behalf of MAG or to represent MAG under duress.
- Reporting any forms of corruption, abuse or fraud committed by colleagues or partners.

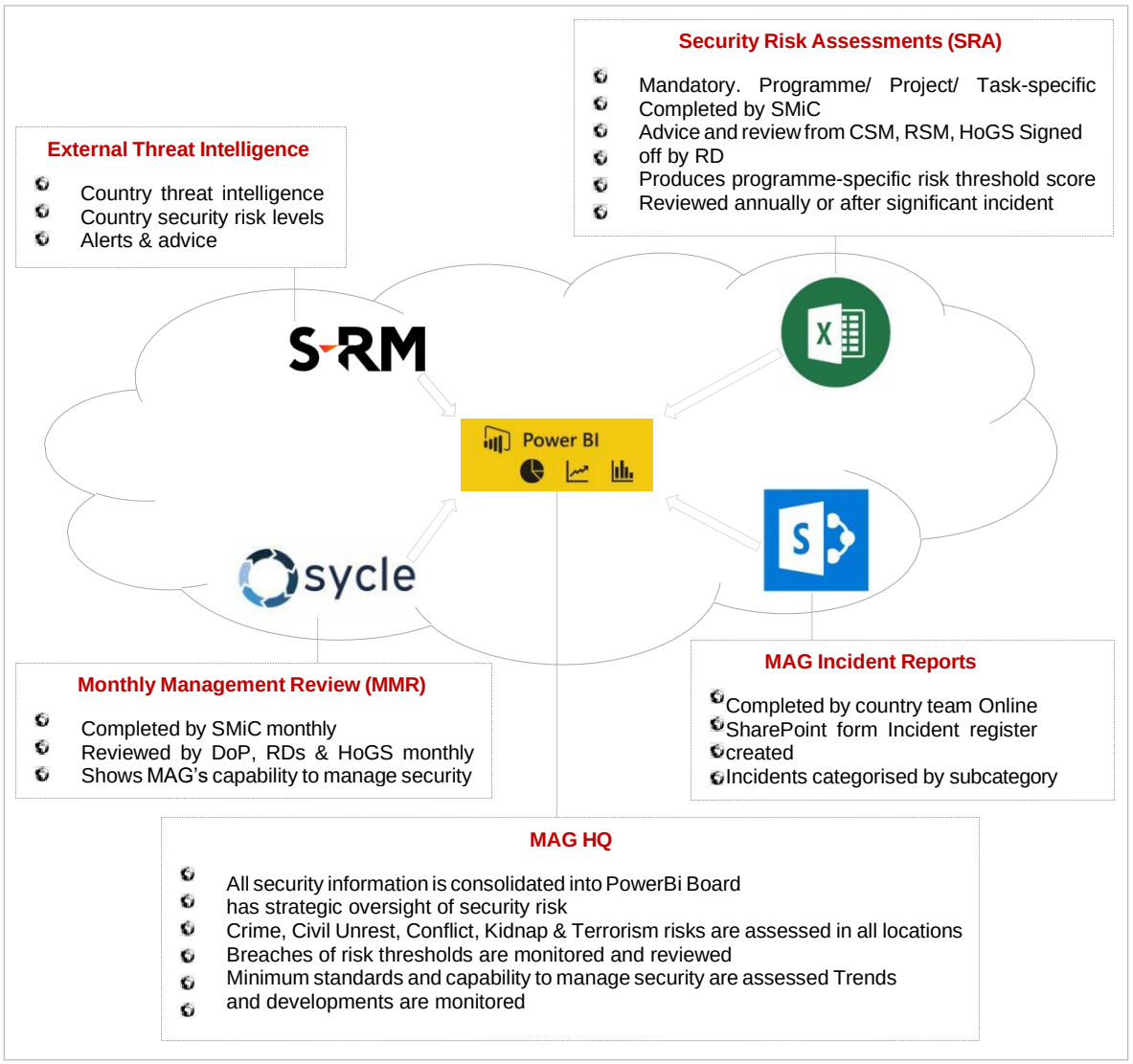
8 – RISK MANAGEMENT

8.1. Organisational Risk Statement:

MAG's position on risk is outlined in the Risk Management Policy.

8.2. Integrated Security Risk Monitoring:

MAG uses an online integrated security risk monitoring system, which aggregates security information from internal and external sources[3] at both field and HQ level. This allows MAG to ascribe risk ratings to programmes, track trends and significant contextual changes, see when risk thresholds are breached and/ or to what extent minimum standards are implemented.



8.3. Security Risk Assessment:

The MAG Security Risk Assessment (SRA) is the basis for assessing and managing all security risks. SRAs are mandatory for all MAG programmes, project sites and new initiatives.

SMiCs are responsible for the SRA, with support provided by CSMs, RSMs, the HoGS and RDs. SRAs will be updated annually, or after any significant change in context. The HoGs and RSMs ensure compliance. Please see 'SRA Guidance' for full details of the SRA methodology.

8.4. Risk Threshold:

At the **strategic level,** as outlined in the diagram above the Senior Leadership Team (SLT), Board of Trustees and HoGS maintain an overview of global security in programmes.

At the **operational level in HQ** the MMR process provides the DOP, RDs and HoGS with a monthly overview of how effectively security is being managed in programmes. Based on the completion of the security section of the MMR the programme will be rated black, red, amber or green. If the programme is rated black or red, then it is not meeting the required minimum standard in security management and the risk threshold has been breached. Immediate escalation to the RD with the support of the RSMs/ HoGS is required to address the issue.

At the **operational level in country** the SRA provides the programme with a risk threshold score based on the countries capacity to handle a major security incident set against the operating context. If this score is breached (after mitigations) then it indicates that the SMiC should immediately escalate the matter to their RD, who with the support of the RSMs/ HoGS will address the issue by reassessing the risk; avoiding the risk; putting in place more robust mitigations, or: improving security management capacity in the programme.

In addition to the above measurable risk thresholds MAG may occasionally opt to tolerate greater risks in pursuit of its strategic objectives, any such decision will only be accepted if MAG assesses that it would be able to effectively manage these risks for a short period of time.

The following indicators would highlight MAG's risk appetite is close to being exceeded, and require Senior Management to be notified for onward decision-making (i.e., whether these risks are to be accepted, avoided, or transferred):

- Any situation that places communities that MAG seeks to serve, or any of its partners in immediate danger because of MAG's presence, services, or activities.
- Where MAG (or any other NGO's, or de-mining agencies working in the same context) require harder 'protective' or 'deterrent' **measures as the norm** for reducing exposure safety and security risks (i.e., where MAG's acceptance cannot be assured).
- Where a credible threat has been made to MAG staff, visitors or consultants that places their safety, security, health or well-being in clear and immediate danger or undue risk.
- Where any high-impact events (e.g., kidnap, effects of conflict, sexual assault

9 - PREPARATION

9.1. On-boarding:

Key security documents will be shared with new staff and consultants as part of their on-boarding. New arrivals will also receive a security induction from the HoGS, RSM and/ or SMiC prior to departure and on arrival in programme. Incoming personnel signal their understanding and acceptance of MAG's security policies and procedures by signing the informed consent form.

Incoming staff will be inducted on MAG's global and country security documents and will be given the opportunity to clarify questions and concerns. They will sign a statement of commitment to confirm they understand and will comply with these security policies and procedures.

9.2. Training:

MAG recognises that preparation of staff to manage their own security and those of their colleagues (for managers) is critical. **All staff, consultants and visitors** are therefore required to complete the UNDSS BSAFE free online security trainings as a minimum. Proof of completion must be sent to the HR department prior to deployment.

It is mandatory for **all staff, consultants and visitors** visiting or deployed to countries with 'HIGH' risk (or above) ratings in the 'OVERALL,' 'WAR,' 'TERRORISM,' or 'KIDNAP' categories[4] to undertake Hostile Environment Awareness Training (HEAT) before deployment. Re-training in HEAT should take place every 3 years.

National Staff should be trained on security risks and standard operational procedures (SOPs). Staff with security management responsibilities should complete security management training (SFPs, CDs, Technical Operations Managers [TOMs], and RDs).

Crisis or incident management teams should complete crisis management training and simulations on an annual basis. SMiCs are to ensure records are kept for the training of their staff and MAG HR department for HQ staff.

9.3. International Travel:
All staff and consultants must follow the 'Guidelines for Travelers' and 'MAG Travel Policy' when traveling internationally or regionally on MAG business. Any international travel by MAG personnel must first be approved by a line manager and travel by HQ staff is to be approved only after the risk assessment form has been completed.

All MAG personnel visiting country programmes are to receive the relevant sections of the security plan with a country briefing pack prior to departure and receive a security briefing on arrival. They are expected to adhere to security plans and come under the authority of SMiCs whilst in programme, adhering to all specific country policies and procedures for the duration of the visit.

10 - PROGRAMMES

10.1. Country Security Plan (CSP):
Every MAG programme with in-country staff and/ or consultants and every MAG Country Office is required to have a Project/ Country Security Plan that follows the approved template. This will normally be written by the SMiC with support from the CSM, RSM and/ or HoGS. The SRA is annexed to the CSP and is also mandatory. This should be developed with the participation of a cross-section of staff, disseminated via trainings and briefings and reviewed on an annual basis by the SMiC, CSM, RSM and/ or HoGS.

10.2. Contingency Plan (CP):
Every MAG programme with in-country staff and/ or consultants and every MAG Country Office is required to have a CP, detailing hibernation, relocation, evacuation, medevac and repatriation planning, procedures, and triggers for initiation. This will normally be written by the SMiC with support from the CSM, RSM and/ or HoGS following the 'Minimum CP Guidelines'.

10.3. Incident Management Plan (IMP):
Every MAG programme with in-country staff and/ or consultants and every MAG Country Office - regardless - of size or capacity is required to have an IMP that follows the approved template.

This will normally be written by the SMiC with support from the CSM, RSM and/ or HoGS. There will be a minimum annual schedule of desktop simulation and/ or crisis training for every programme.

11 – INCIDENT REPORTING AND MANAGEMENT

11.1. Incident Reporting:
Security incidents should be reported to SMiCs as soon as possible using the MAG security incident report form. In line with the standard operating procedure 6 ('SOP6'), SMiCs are to forward incident reports to RDs, copied to the HoGS, and records are to be maintained. CDs will manage security incidents with the support of their Incident Management Teams (IMTs) and advice from the RSMS, HoGS and RDS.

11.2. Crisis Management:
MAG recognises the possibility of a critical incident occurring. Examples of a critical incident include but are not limited to kidnap, hijack, arrest, and detention. MAG's 'Crisis Management Plan' outlines the procedure for managing a critical incident. The objectives of any critical incident response must be to:

- Map out a clear plan for management and resolution of the incident.
- Prevent further harm to and ensure the safety of affected staff during the incident.
- Support affected staff after the incident.
- Assure next of kin of a comprehensive and effective response.
- Ensure internal and external effective communications during an incident.
- Ensure organisation and program continuity during the incident.

It is the responsibility of the SMiC to ensure that **all programmes** develop their own incident management plans (IMPs) using the IMP template.

11.3. Kidnap:
In the event of a kidnap MAG will convene its Crisis Management Team, who will guide the incident response and take all possible legal steps to secure the individual's release as swiftly as possible. MAG will engage with the government of the kidnapped individual and use the services of necessary experts to assist in the response. MAG

will continue to pay an individual's salary while they are detained and will extend all possible support to the individual's next of kin during the incident. Following an incident MAG will ensure all necessary medical and psychological support is provided to the individual including immediate repatriation.

This is applicable to international staff and consultants while deployed out of their country of domicile on MAG business. It applies to national staff and consultants during working hours unless the incident occurs outside out of working hours and is as a direct result of their association with MAG. It will apply 24 hours when any member of staff travels away from their place of residence on MAG business.

12 - MINIMUM STANDARDS

12.1. Programmes (MS-P):

CDs and SMiCs *must* ensure the implementation of the following minimum standards in programmes:

Reference	Minimum Standard
MS-P1	Country and project specific Security Risk Assessment - reviewed at least once every 6 months (for high-risk locations), once a year (low and medium) or following an incident or significant change in the operating context.
MS-P2	Country Security Plan based on approved template.
MS-P3	Contingency Plans for hibernation, relocation, and evacuation.
MS-P4	Medical emergency and evacuation plan.
MS-P5	Country specific incident management plan.
MS-P6	Site Security Assessment for all offices, accommodation, and other sites.
MS-P7	Primary and secondary communications methods.
MS-P8	Staff and visitor completion of UNDSS BSAFE online course within the last 2 years.
MS-P9	Country specific security induction for all staff.
MS-P10	Staff and visitor completion of HEAT within 3 years and before arrival in countries with 'HIGH' risk (or above) ratings in the 'OVERALL,' 'WAR,' 'TERRORISM,' or 'KIDNAP' categories.
MS-P11	Personnel tracking mandatory for staff in or visiting countries with 'HIGH' risk (or above) ratings in the 'WAR,' 'TERRORISM,' or 'KIDNAP' categories or when recommended by the security team.
MS-P12	For all 'off MAG platform travel' where MAG staff or consultants are to be hosted by another agency or organisation the MAG Host Agency Security Questionnaire *must* be shared with and completed by the hosting organisation in advance of travel.
MS-P13	Any use of armed protection *must* be requested in advance and only used if first approved by the CE.
MS-P14	For all travel to countries where MAG has no, or limited physical presence with 'HIGH' risk (or above) ratings in the 'OVERALL,' 'WAR,' 'TERRORISM,' or 'KIDNAP' categories, or where the RSM or HoGS deem it necessary, a Travel Risk Assessment (TRA) *must* be completed and submitted to the RSM, RD and HoGS for approval in advance.

12.2. International Travel (MS-IT):

All international travelers *must* adhere to the following minimum standards:

Reference	Minimum Standard
MS-IT1	Travel approved by line manager and recipient SMiC on its necessity and acknowledgement of the safety and security risks involved.
MS-IT2	Traveler read pre-deployment briefing pack and received 1:1 briefing for all countries with 'high' and above risk rating.
MS-IT3	Completed proof of life and informed consent forms.
MS-IT4	Completed UNDSS BSAFE online course within the last 2 years.
MS-IT5	Completed approved HEAT training within last 3 years if travelling to a high-risk country (or above).
MS-IT6	Consult a medical practitioner / travel clinic for vaccinations and anti malarials.
MS-IT7	Current visa.
MS-IT8	Check-in with an appointed MAG contact on arrival and departure from the destination(s) they are visiting.
MS-IT9	Issued with a reliable form of communications upon arrival in-country.
MS-IT10	Traveler must have own insurance for any personal travel taken at conclusion of business travel.
MS-IT11	For all 'off MAG platform' travel where MAG staff or consultants are to be hosted by another agency or organisation the MAG Host Agency Security Questionnaire *must* be shared with and completed by the hosting organisation in advance of travel.
MS-IT12	For all travel to countries where MAG has no, or limited physical presence with 'HIGH' risk (or above) ratings in the 'OVERALL,' 'WAR,' 'TERRORISM,' or 'KIDNAP' categories, or where the RSM or HoGS deem it necessary, a Travel Risk Assessment (TRA) *must* be completed and submitted to the RSM, RD and HoGS for approval in advance.

12.3. Incident Reporting (MS-IR):

Reference	Minimum Standard
MS-IR1	Incident reporting form and process in place in every country programme that enables 24h reporting of an incident.
MS-IR2	Staff briefed on this on at least a 6-monthly basis by SMiC/ RSM/ CSM.
MS-IR3	Verbally reported incidents and near-misses are written into an Incident Report Form within 48 hours of first report.
MS-IR4	Incident review and lessons learned conducted within 7 working days of the security incident report being submitted.

12.4. Crisis Management (MS-CM):

Reference	Minimum Standard
MS-CM1	Global and country-specific crisis management plans in place and reviewed after every incident or annually.

MS-CM2	Crisis Management Team (CMT) is established in HQ with primary and alternates identified.
MS-CM3	CMT trained at least once every year.
MS-CM4	Incident Management Team (IMT) is established in every country with primary and alternates identified.
MS-CM5	IMT trained at least once every year by CSM/ RSM/ HoGS.

13 - REVIEW

The security policy will be reviewed on an annual basis or following any major security incident taking into consideration any recent developments in sectoral best practice.

MAG 24 01 Insurance Services – Relevant MAG Policies

RISK MANAGEMENT POLICY (last approved October 2022)

Purpose of this Policy

Purpose of this Policy MAG's Board of Trustees and Leadership Team recognise that risk management is an integral part of good management practice and an essential component of good governance. Risk management adds value to the operations and activities of the organisation by identifying and mitigating events and threats that could otherwise impede the achievement of our objectives and/or the continued effectiveness of MAG's delivery of services to our beneficiaries and stakeholders. Ultimately, an effective risk management framework, underpinned with a strong culture of risk awareness, will enable MAG to deliver on our Vision and Mission.

The purpose of this Policy is to ensure that:

- There is an organisation wide commitment and responsibility for risk management.
- Risks are identified, assessed and managed in a coordinated and consistent manner.
- A positive risk culture is developed and maintained across the organisation.
- Risk management principles and activities are embedded across the organisation.
- The Board of Trustees can effectively discharge its reporting obligations under Charity Commission regulations, the SORP (Statement of Recommended Practice) and UK Company Law.

Link to Values

This policy particularly links to MAG's value of Integrity. Management of risk is very often about doing the right thing – which is ultimately around good governance. Management of risk can create the organisational culture environment that supports the organisation with our other values of Expert, Determined, Compassionate and Inclusive.

Responsibilities

Responsible Entity	Responsibilities
Board of Trustees	The Board is ultimately accountable for the management of the risk exposures within MAG. Specifically, the Board shall: • Define the Organisation' risk appetite • Establish the Organisation's risk criteria • Regularly monitor and review risk as part of a standing item on the consideration of governance issues. • Promote a risk management culture within the organisation
Board Committees (AFRC, GNRC, HSC)	• AFRC is to provide oversight of MAG's risk management framework to ensure that it is fit for purpose. • All committees to liaise with management in monitoring key risks and, where appropriate, report to the Board to provide assurances concerning the management of risks within
MAG Chief Executive	• Responsible for ensuring that risk management activities are carried out effectively within the organisation and for promoting a culture that encourages strong risk management. • Appoint Risk Owners. • Report to the Board sub-committees on material changes in risk, risk issues arising, and progress on action plans designed to reduce risk.
Director – Governance and Business Transformation	• Represent the risk management function at Leadership Team level • Lead on the coordination of the three lines model to ensure that compliance and audit functions provide necessary risk assurance • Support the Chief Executive in their responsibilities
Head of Risk Management	• Coordinate the development and delivery of the Risk Management framework. • Ensure integration, alignment and consistency of the risk management function across all departments

	• Undertake analysis, reporting and communication of risk. • Strengthen organisational capacity development and training of the risk management framework and process. • Assist risk and control owners in meeting their requirements
Risk Owners	The Risk Owner is the person assigned the responsibility for the day-to-day management of a risk. Risk Owners are responsible for the following: • Overall coordination of the management of the risk including: • Assurance that controls are effective • Treatments are completed • Monitoring of the environment to identify if there are any indicators the risk might eventuate • Reporting
Control Owners	Control Owners are assigned the responsibility for the day-to-day management of a control. Control Owners are responsible for: • Maintaining oversight of the effectiveness of the control, • Reporting any changes to effectiveness to the Risk Owner
Treatment Owners	Treatment owners are responsible for the following: • Implement the treatment as directed • Providing ongoing status of the risk treatment • Reporting any issues that may impact completion within timeframes • Reporting when complete
All Staff	Diligently identify, assess risks and implement mitigating actions to reduce the risk where required. Report incidents through appropriate channels.

Definitions

MAG applies the following definitions:

Term	Definition
Risk	A possible event or incident that, if it occurs, will have an impact on the organisation's objectives.
Risk Management	The systematic and coordinated process that enables an organisation to make informed decisions as to the actions to be taken in relation to the possible events or incidents that, if they occur will impact on organisational objectives.
Risk Management Framework	The totality of systems, structures, policies, processes and people that identify, measure, monitor and mitigate risk.
Target Level of Risk	The level of risk that the organisation is willing to accept

Policy statements

The following policy statements are to be adhered to by all MAG personnel.

- Risk shall be considered in any planning process undertaken within MAG.
- The criteria to be used for risk assessments shall be those detailed in the MAG Risk Management Procedures.
- Accountability for activities within the Risk Management Framework will be allocated to those with the levels of authority necessary for decision making.
- All risks shall be recorded and updated within MAG's centralised risk register.
- All personnel with roles and responsibilities within the Risk Management Framework should receive appropriate training.
- Those allocated responsibility for managing risks or being accountable for critical controls shall establish and maintain appropriate monitoring and reporting mechanisms.
- Risks shall be reported to the Board quarterly.
- Adjustments to the risk register, including addition of risks, removal of risks and/or changes to risk level are to be endorsed by the assigned Committee prior to being approved by the Board.

MAG 24 01 Insurance Services – Relevant MAG Policies

Risk Management Framework
MAG's overall approach, methodology and criteria for risk management are outlined and described in the Risk Management Framework and Risk Management Procedures documents. The Risk Management Framework is a governance document that supports the implementation of this policy and should be consistent with the International Standard, ISO 31000:2018 (Risk Management - Guidelines).

- The Risk Management Framework sets out the structure for all requirements to effectively manage risk in the organisation
- The Risk Management Plan outlines the steps taken to implement the framework and is used to monitor progress of the framework implementation.
- The Risk Management Procedures outline the operating model, process and criteria to be used to identify, assess, manage, monitor and report risk.

Risk Appetite Statement
Every organisation is exposed to a multitude of risks and ultimately the pursuit of zero risk is unattainable. MAG does not perceive the existence of risk as a barrier in pursuing and achieving our aims and objectives. Our aim is to manage risk – by making informed decisions in understanding how we are exposed to certain risks and being assured that appropriate control measures are in place.

MAG acknowledges that not all risks are the same and there may be times where we will make informed decisions to accept certain risks at levels that are higher than our defined target levels. The criticality of programming needs to benefit people in need, is a key criterion MAG will consider in accepting higher levels of risk.

Overall, MAG will take a balanced posture towards People, Financial and Programming risks and a conservative posture towards Reputation and Legal and Regulatory risks.

Management Commitment
The mandate for risk management comes from the Board of Trustees and Leadership Team and are committed to ensuring sustainable and effective risk management within MAG by

- Ensuring that risk management is an integral part of MAG's planning and decision-making processes.
- Establishing is a consistent approach to the management of risks across MAG.
- Defining clear roles, responsibilities and accountabilities.
- All staff with risk management roles and responsibilities are provided with the necessary authority and skills to undertake these responsibilities.
- Ensure that the resources necessary to achieve the policy outcomes are allocated.

Governance of Risk
To ensure the effectiveness of the organisation's risk management framework, MAG has adopted the 'Three Lines Model'. The three lines model articulates the roles and relationships of:

- Organisational Management (1st and 2nd Lines) – to effectively manage and monitor risk
- Independent Review (3rd Line) – to provide assurance of risk management actions
- Governing Body – to provide oversight and maintain accountability The application of the 3 lines model, with in MAG's governance structures.

Monitoring

- The submission of – and requirement to update, Country Risk Assessments will be monitored
- The submission of appropriate Risk Reports to the Board of Trustees.

MAG 24 01 Insurance Services – Relevant MAG Policies

SAFEGUARDING POLICY (last approved January 2022)

Purpose of this Policy

MAG believes that everyone we come into contact with, regardless of age, gender identity, disability, sexual orientation or ethnic origin has the right to be protected from all forms of harm, from sexual exploitation, abuse, bullying and harassment. MAG will not tolerate exploitation, abuse or bullying and harassment by staff or associated personnel and applies a zero-tolerance approach to any breach of this and associated policies.

MAG further defines safeguarding as a set of standards, policies and procedures that are intended to safeguard everyone who works in, or comes into contact with the organisation. The scope of this includes behaviour or any act that involves one person using their power or influence over another person; ensuring staff, operations and programmes, do no harm, or expose individuals to sexual exploitation, abuse or neglect, whilst protecting staff from inappropriate behaviour such as bullying and all forms of harassment. All relevant policies are detailed in associated policies.

This policy addresses for MAG the following areas of safeguarding:

- Protection from sexual exploitation and abuse
- Bullying and harassment
- Adult safeguarding
- Child safeguarding
-

MAG commits to addressing safeguarding throughout its work, through the three pillars of prevention, reporting and response.

The purpose of this policy is to protect people, particularly children, vulnerable adults and communities in receipt of assistance, from any harm from sexual exploitation, abuse and neglect that may be caused due to their coming into contact with MAG. It also includes harm caused by bullying and harassment in the workplace.

Harm in this policy may arise from:

- The conduct of staff or personnel associated with MAG
- The design and implementation of MAG's programmes and activities.

This policy lays out the commitments made by MAG and informs staff and associated personnel1 of their responsibilities in relation to safeguarding.

This policy does not cover:

- Safeguarding concerns in the wider community not perpetrated by MAG or associated personnel

Link to Values

MAG's vision is a safe future for women, men and children affected by violence, conflict and insecurity; our mission is to save lives and build safer futures.

We recognise that our behaviour has an impact on others and on MAG. By adopting our values – determined, expert, integrity, compassion and inclusive, and following the Policy on Personal Conduct, we can all contribute towards MAG's vision and mission.

Responsibilities

This safeguarding policy applies to:

- All staff contracted by MAG
- Associated personnel whilst engaged with work or visits related to MAG, including but not limited to the following: consultants; volunteers; contractors; programme visitors including journalists, celebrities and politicians[1] See 'Responsibilities' for definition of associated personnel

Definitions

What is safeguarding?

MAG 24 01 Insurance Services – Relevant MAG Policies

Safeguarding broadly means protecting peoples' health, wellbeing and human rights, and enabling them to live free from harm, abuse and neglect. MAG understands safeguarding to mean protecting children and adults, from harm that arises from coming into contact with our staff, operations or programmes. MAG defines safeguarding as 'any behaviour or act that involves one person misusing their power or influence over another person'. MAG aims to protect everyone who comes into contact with us from:

i. Misuse of power or influence over another person
ii. Harm from sexual exploitation, abuse, bullying and harassment
iii. Inappropriate, exploitative or degrading behaviour

Further definitions relating to safeguarding are provided in the glossary below.

MAG Safeguarding Approach

Our approach to safeguarding is survivor centred, within an organisational culture that aims to prevent harm and abuse from occurring, but which responds quickly and thoroughly when it does happen. We will learn from experience and share good practice throughout the organisation.

We will work towards:

Survivor support and enhanced accountability

- Protecting the dignity and safety of the people our work serves
- Ensuring survivors are central to our safeguarding response
- Being transparent and sharing progress
- Ensuring rigorous, accessible, and inclusive reporting and complaints processes

Cultural change

- Driving cultural change and addressing structural inequalities from the top
- Ensuring consistency in approach • Collaborating to improve employment practice
- Applying our own standards (see below) international human rights law, alongside internationally recognised UN standards and sectoral best practice
- Collaborating with others in our sector to advance global safeguarding practice
- Ensuring policies and practice address the needs of vulnerable groups

Organisational capacity and capability

- Improving and sharing expertise of staff, partners and agencies with whom we work /collaborate
- Equalise relationships between organisations delivering and receiving assistance

Standards based approach

MAG has developed and will apply 6 standards to safeguarding:

1. **Safe culture:** the organisational culture for safeguarding MAG's workplace is built on respect, tolerance, diversity and inclusion that delivers a respectful environment for all staff, and supports staff to create a safe environment in which to deliver the organisation's work.
2. **Safe People:** recruitment, induction, training, staff conduct and equal opportunities. MAG's HR policies, processes and systems set out, and implement, organisational responsibilities around the employee lifecycle. Ensure staff with responsibilities for safeguarding are appointed and skilled to undertake their roles
3. **Safe programmes:** risk assessments are conducted and partnership agreement are in place and are designed to prevent harm and abuse to the people with whom we work and the communities in which we work. National context is understood and reporting mechanisms are clear.
4. Safe communications: use of information and images in MAG's communications activities feature appropriate images and stories of communities and children and ensure that they are not exposed to harm and abuse.
5. **Safe response:** MAG treats any allegations related to safeguarding extremely seriously. We strive to learn and identify areas in which we could improve, and welcome feedback from any stakeholders. We commit to respectfully listening and supporting individuals who want to raise a concern or make a complaint. We will also ensure that genuinely held concerns will be thoroughly investigated.

6. **Safe Governance:** MAG's governance is based on our values, and promotes transparency, probity and accountability

Roles and responsibilities
The Safeguarding Policy places a number of responsibilities on various groups of people involved in MAG's work. These are as follows:

MAG's Board of Trustees: have a duty of care to ensure that appropriate policies and procedures are in place to prevent abuse from taking place and to appropriately manage any concerns.

They also have a responsibility to ensure that all appropriate issues are reported in line with best practice and to appoint a Safeguarding Trustee Focal Point who will provide subject matter expertise and has delegated responsibility on behalf of the Board for ensuring that MAG maintains effective safeguarding policies, procedures and practices.

The Board of Trustees also have responsibility for reporting to the Charity Commission and any other relevant regulatory body in the UK or other location.

Board Committees:
Delegated responsibility rests with the following board sub-committees in relation to safeguarding:

- **The Governance Nominations and Review Committee (GNRC)** maintains oversight of MAG's incident reporting to the Charity Commission and any other relevant regulatory bodies. The committee will ensure that incident reporting practice is in line with the Commission's expectations and with sector good practice.

- **The Health, Safety, Security and Safeguarding Committee (HSC)** provides strategic oversight for all aspects of safeguarding at MAG and will ensure that policies and procedures are up to date, effective, appropriate and fully implemented. The Chair of the HSC and the Safeguarding Trustee Focal Point will review the Safeguarding Register and will ensure that appropriate action is taken in relation to any issues.

The Chair of both GNRC and HSC will be notified immediately of any potentially serious incidents as soon as they are reported through appropriate channels. This will enable the GNRC to ensure that all reporting to the Charity Commission takes place within recommended timescales. The HSC will be responsible for fulfilling any further reporting requirements including responding to requests for information.

MAG's Leadership:
The Leadership Team will ensure:

- Build a culture of openness to enable issues and concerns about safeguarding to be raised and discussed
- Build a sense of accountability between staff so that potential poor or abusive behaviour can be challenged
- Maintain a reputation of robust standards and high standards of working

MAG's Safeguarding Lead reports to the Director of People and Culture, who in turn reports to the Chief Executive.

Management responsibilities: all managers have a particular responsibility to uphold the standards within each policy and to set an example ensuring that a culture of dignity and respect is maintained. Managers should encourage an open and transparent way of working that facilitates a strong safeguarding culture within and between teams.

As well as upholding standards themselves, managers are expected to ensure that all staff understand the provisions clearly and challenge any unacceptable behaviour. In addition, managers must ensure that any reports or complaints are taken seriously and investigated promptly and thoroughly. All MAG programmes have

a responsibility for ensuring that standards contained within each policy are upheld in each location and policies are translated into the relevant local language and understood by all.

All individuals: creating a safe working environment at MAG is everyone's responsibility and failure to act on concerns or disclosures relating to sexual harassment, abuse and exploitation is not an option.

MAG recognises that often employees will be the first to know when there is cause for concern. All staff and partners have a responsibility to act with due care and attention to safeguard the wellbeing of every person, specifically those who are vulnerable. All individuals should remain vigilant, be prepared to take action and understand what to do in the event there is a concern to raise. Therefore, all MAG representatives should understand and abide by the standards set out within this policy.

All MAG employees are obliged to report any suspicions of sexual exploitation, abuse or harassment of others. Failure to report suspicion of abuse relating to someone else to a relevant person is a breach of MAG's policy, and could lead to disciplinary action being taken. If necessary, this report can be made anonymously. Although we strongly encourage reporting through the available channels, for the avoidance of doubt, there is no obligation placed on any individual to report any incident that has happened to them. However, where there is a clear legal requirement placed on MAG to report, the decision will be made by MAG in consultation with the alleged subject of abuse.

Additionally, MAG staff and associated personnel are obliged to:

- Contribute to creating and maintaining an environment that prevents safeguarding violations and promotes the implementation of the Safeguarding Policy
- Report any concerns or suspicions regarding safeguarding violations by a staff member or associated personnel (and where necessary the actions of non MAG staff, where there is concern and where it relates to MAG)

Prevention

MAG will:

- Ensure staff and personnel associated with MAG are given every opportunity to become aware of the standards and expectations that we have set ourselves • Design and undertake all its programmes and activities in a way that protects people from any risk of harm that may arise from their coming into contact with MAG.
- Implement stringent safeguarding procedures when recruiting, managing and deploying staff and associated personnel
- Ensure staff receive appropriate training and support on safeguarding – all staff will receive further information during their induction and will attend an annual refresher training • Provide clear systems on how to report concerns as soon as they are identified or suspected
- Comply with international standards in relation to safeguarding

Reporting and Response

MAG will ensure that safe, appropriate, accessible means of reporting safeguarding concerns are made available to staff and the communities we work with.

MAG recognises that the standards outlined in each policy can only be upheld if strong reporting channels exist and are understood by all. As such, each policy outlines how concerns should be raised and what action may be taken where incidents or concerns arise. For further information refer to policies listed below.

The Policy on Personal Conduct states that it is the duty and responsibility of all managers, employees and representatives to report any suspicions or incidences of inappropriate behaviour. All MAG employees are obliged to report any suspicions or incidences of inappropriate behaviour towards others. This can be done without sharing details of cases where information has been shared in confidence. Failure to report suspicion of abuse relating to someone else to a relevant person is a breach of MAG's policy and could lead to disciplinary action being taken. Although we strongly encourage reporting through the available channels, for the avoidance of doubt, there is no obligation placed on any individual to report any incident that has happened to them.

However, where there is a clear legal requirement placed on MAG to report, the decision will be made by MAG in consultation with the alleged subject of abuse.

MAG recognises that not all complainants may be willing to reveal their identity. This does not necessarily have any bearing on the truth of the complaint, but may be an indication of fear of reprisal. Anonymous complaints will be treated as seriously as complaints where the identity is known. The substance of the allegation should still be reported to the SMiC along with the identification of the alleged perpetrator, if known. The wish for anonymity only applies to the complainant and not to the subject of the complaint.

In addition, rumours must not be left unchecked and may be an early warning of a greater problem. MAG will take rumours seriously and they must be reported and investigated.

Support for Survivors: MAG will always offer support to survivors, regardless of whether a formal internal response is carried out (such as an internal investigation). Support can include specialist psycho-social counselling, and/or access to other specialist and appropriate support as needed (medical and where possible legal). Survivors can choose if and when they would like to take up the support options available to them. On hearing a complaint or concern, the priority is to ensure and check if the complainant is in need of mental or physical support. All further action will only be taken with the survivor's agreement or consent unless they are a child or vulnerable adult.

Raising a complaint: anyone can raise a concern or make a complaint to MAG about something they have experienced or witnessed. Reporting/complaints mechanisms are encouraged at all levels of the organisation. Complaints or concerns can be made in any language and arrangements will be made for a confidential translation. In addition, anonymous complaints are accepted and MAG will investigate as far as is reasonably possible.

Safeguarding Focal Points: MAG's global network of Safeguarding Focal Points support MAG to prevent and respond to sexual harassment, abuse and exploitation by receiving concerns and forwarding these to the team, raising awareness and promoting best practice. Focal points are not required to investigate concerns or complaints themselves.

Community complaints: communities will be informed of how they can make a complaint or raise a concern if necessary. Arrangements will vary between each programme.

Complaints about partners: if MAG receives a complaint about a partner organisation, it will expect the partner to respond quickly and appropriately. MAG will assist the partner to ascertain its obligations under local law to refer the matter to the police or other statutory authorities for criminal investigation. Where appropriate, MAG will work with the partner to address the issue through an appropriate independent investigation. If the outcome is that abuse has occurred, ongoing work with the partner cannot involve the individual(s) concerned. If there is reason to believe that an allegation of abuse has been dealt with inappropriately by a partner then they risk withdrawal of funding or ending the relationship (including networks and consortia).

Complaints from outside of MAG: can be sent in writing to reporting@maginternational.org or directly to the Leadership Team or anyone on the Board of Trustees. This can include someone in receipt of MAG's assistance (beneficiaries); other people directly affected by MAG policies, actions or our staff; partners and their staff (humanitarian partners and contractors); MAG staff or any visitor to a MAG site or office. The email address is monitored by the Company Secretary and the email received will be forwarded to the appropriate people with oversight by whoever the email was addressed to.

Statutory and external reporting: the decision about whether to refer an allegation to local police or statutory authorities is made by the person who it is alleged has been the subject of abuse ("the victim/survivor" - who may or may not be the complainant). MAG will support the victim/survivor and/or complainant regardless of whether they wish to report to local police/statutory authorities or not. However, MAG's approach will always be to comply with reporting obligations under local law. Where there is a clear legal requirement placed on MAG to report, this decision will be made by MAG in consultation with the alleged subject of abuse. If someone's life

is in danger or the matter relates in any way to a child or adult at risk, then some decisions may have to be taken by MAG (for example, to contact the police or statutory authority).

The principle of 'survivor led' must be balanced against risk and protection of vulnerable groups in every instance. If the victim/survivor is a child or adult at risk, then decisions about their welfare may have to be made by others. However, as far as is possible and appropriate they will be engaged in the conversation about their own welfare.

Regulatory and donor reporting: MAG's regulatory authorities and donors have different reporting mechanisms in relation to safeguarding incidents. All incidents that involve national, international staff or partners, must be reported immediately to the Regional Director and HQ HR who will be able to advise accordingly.

Implementation of the safeguarding policy will be supported by:

- **Staffing** – a senior level full time safeguarding position will be in place, safeguarding focal points will be recruited across the organisation, safeguarding responsibilities will be included in job descriptions. All staff with responsibility for implementation will receive training.
- **Prevention** – safeguarding will be integrated into all aspects of MAG's work and systems, including awareness raising from application stage and continuous throughout an employee's employment at MAG. Risk assessment will be considered at all levels including when working with partners, when designing new programmes and setting up new operations at local and national level.
- **Reporting and responding mechanisms** – steps for raising or reporting safeguarding concerns will be known to all, investigation and incident management procedures are clear and understood: duties and responsibilities are clear for those who have safeguarding responsibilities, in particular managers, HR teams and focal points
- **Implementing, maintaining, reviewing and monitoring** the safeguarding policy – training and capacity building of staff and partners, monitoring and reporting and continuous review of the policies
- **Budget** – will be available to support with organisation wide safeguarding activities.

Monitoring

To ensure this policy remains relevant and appropriate, it will be reviewed every three years, alongside the associated policies. Progress on implementation will be reported to the Board sub-committees and Board every quarter. Programmes report to HQ on safeguarding activities twice a year. All case management is monitored and reported as appropriate to Trustees through the SIR log. The Safeguarding Trustee Focal Point and Safeguarding Lead will meet monthly.

Contacts

For more information on this policy please contact safeguarding@maginternational.org.

MAG 24 01 Insurance Services – Relevant MAG Policies

FINANCIAL MISCONDUCT (last approved January 2021)

Policy Statement
Acts of financial misconduct and crime threaten funds donated to MAG which are intended to save lives and help build safer futures for MAG's beneficiaries. MAG is committed to the highest ethical standards and has zero tolerance of financial misconduct, financial crime and all other forms of criminality.

Scope
MAG's Financial Misconduct Policy ("Policy") sets out MAG's mandatory requirements to prevent, deter, detect, report and investigate financial misconduct and acts of criminality.

This Policy applies to MAG's trustees, employees, contractors, consultants and partner organisations acting on MAG's behalf, interns and volunteers, and accompanying partners and family members of international staff (collectively "MAG Staff and Associates").

The MAG Financial Misconduct and Crime Policy Handbook ("Handbook") provides the procedures supporting the application of this Policy. Part A of the Handbook provides guidance for all MAG Staff and Associates on raising concerns about financial misconduct or crime. Part B of the Handbook describes MAG's required procedures for the conduct of financial misconduct and crime investigations.

Definitions
Financial misconduct
Non-conformance with MAG's ethical standards and internal financial policies, controls and procedures, whereby such behaviour would risk the loss, misappropriation or misreporting of MAG's and donors' assets and funds.

Conflicts of interest can also lead to financial misconduct.

Financial crime
Acts which break national or international laws and regulations and involve intentional illegal and dishonest activities to misappropriate, redirect and / or wrongfully gain assets and funds. Illegal acts which constitute financial crime are:

- theft, embezzlement, extortion;
- fraud, false accounting, forgery;
- bribery, corruption and money-laundering;
- terrorist financing and violation of economic sanctions;
- tax evasion.

Further explanations of the above financial crimes are provided in the Financial Misconduct and Crime Policy Handbook.

REQUIREMENTS
MAG Staff and Associates shall:

- protect MAG's and its donors' funds, property and assets, acting appropriately to ensure that they are not misappropriated, misdirected, lost, misused or damaged;
- ensure that all financial transactions are properly authorised, recorded, reported and archived as required by MAG's financial framework and relevant laws, regulations and donor requirements;
- abide by all relevant laws against financial crime;
- report immediately any suspicion of financial misconduct, crime or non-compliance with this Policy, following the guidance in the Handbook and MAG's Reporting Malpractice & Raising Concerns ("Whistleblowing") Policy and Procedure;
- complete all MAG required training for the prevention of financial misconduct and crime.

MAG's management shall:

- investigate all suspicions of financial misconduct and financial crime in accordance with the Handbook's procedures;
- reserve the right to search all MAG property and review all data stored on MAG systems if there are reasonable suspicions of financial misconduct or crime;
- report suspicions of financial crime and misconduct to MAG's Audit and Finance Committee, MAG's Board, its donors, the UK Charity Commission and national authorities when required;
- inform and work collaboratively with local and / or international law enforcement bodies in relation to any related investigations and prosecutions;
- take proportionate action against those who commit financial misconduct or crime, up to and including dismissal of MAG Staff and Associates and termination of contracts with partners and third parties;
- seek to recover any losses wherever viable.

INTER-AGENCY PROCUREMENT GROUP (IAPG)'S CODE OF CONDUCT

The IAPG endorses the UN Global Compact and has adopted the ten principles as our Supplier Code of Conduct.

Human Rights

- Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights; and
- Principle 2: make sure that they are not complicit in human rights abuses.

Labour

- Principle 3: Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining;
- Principle 4: the elimination of all forms of forced and compulsory labour;
- Principle 5: the effective abolition of child labour; and
- Principle 6: the elimination of discrimination in respect of employment and occupation.

Environment

- Principle 7: Businesses should support a precautionary approach to environmental challenges;
- Principle 8: undertake initiatives to promote greater environmental responsibility; and
- Principle 9: encourage the development and diffusion of environmentally friendly technologies.

Anti-Corruption

- Principle 10: Businesses should work against corruption in all its forms, including extortion and bribery.

For more information on the UN Global Compact and to sign up, please visit www.unglobalcompact.org/participation

Disclaimer

Individual suppliers entering into procurement and contracting processes with IAPG members will have to agree to organisation-specific terms and conditions, which supersede this code of conduct.

MAG 24 01 Insurance Services – Relevant MAG Policies

MODERN SLAVERY STATEMENT (last approved April 2023)

Introduction
Modern Slavery is the term commonly used to refer to illegal exploitation of people for personal or commercial gain. Victims often find themselves trapped, against their will, in situations of domestic servitude, sexual exploitation, forced marriage, forced criminality, and forced labour often as the result of coercion, bribery, deceit or human trafficking.

At MAG, we value not only our own people, but those whom we serve and work with; our beneficiaries and their communities, and so must be vigilant in our recruitment, partnership arrangements and supply chains. Our response to modern day slavery embodies our values.
We will:

- Raise awareness and understanding across our programmes and teams to support and encourage the reporting of any concerns about our supply chain activities
- Understand our exposure to modern slavery risk and put in place appropriate controls
- Ensure our employment and remuneration practices are fair and transparent across all territories; and
- Promote and enforce ethical standards with our suppliers and be vigilant that suppliers don't engage in any practice that could undermine any aspect of human dignity.

1. Organisation Structure and supply chains

MAG is a charity limited by guarantee and is governed by a non-executive Board of Trustees, operating from a head office in Manchester and currently delivering activities in countries across Africa, Asia, Latin America, the Middle East and Europe.

We employ over 5,800 staff, 97% of whom are local nationals. We work in partnership with many different types of organisations to deliver our work, including other international NGOs, local and national NGOs, academic institutions, and state institutions.

Since 1989, MAG has helped over 20 million people in 70 countries rebuild their lives and livelihoods after war. We find, remove, and destroy landmines, cluster munitions and unexploded bombs from places affected by conflict. MAG also provides education programmes, particularly for children, so people can live, work, and play as safely as a possible until they clear the land. In addition, we work in communities to reduce the risk of armed violence through weapons and ammunition management programmes which keep guns and munitions safe and secure. Our income for the 12-month period ended 31st December 2022 was £90m.

2. Key initiatives

Some of the key initiatives that MAG has in progress that contribute towards addressing modern slavery are:

- Enhancing supplier due diligence
- Supplier management training
- Embedding safeguarding practices across the organization

3. Risk Management

MAG systematically considers our exposure to the risks of modern slavery across the organization within our risk management framework. Working across a wide range of geographical locations and using a mixture of local and international supply chains there is a level of complexity that MAG needs to consider ensuring that we are compliant with the principles of the Modern Slavery Act 2015. To navigate through this complexity MAG has a range of control and mitigation measures in place to minimise any possible occurrences of modern slavery.

4. Risk control and mitigation

The policies and procedures outlined below are some of the key control measures that MAG has in place to reduce the likelihood and impact of modern slavery in our organization. Through the implementation of these control measures MAG is satisfied that we are compliant with the Modern Slavery Act 2015.

i) Recruitment and Selection Policy: Ensures that all recruitment decisions are made fairly and transparently; that processes are free from all types of unlawful or unfair discrimination and bias to ensure that equality of opportunity is maintained for all candidates and prospective candidates.
ii) Remuneration Policy: seeks to ensure that we pay our people in line with the respective laws, cultures and market conditions of the relevant country context. iii) Financial Misconduct and Crime Policy: MAG is committed to the highest ethical standards and requires all staff, consultants, trustees, contractors, partners, agents, and other associates to be familiar with and comply with both the detail and the spirit of this policy. We have established a 'zero tolerance' culture across the organisation to financial misconduct and crime and all forms of corruption and criminality, including slavery, human trafficking, and exploitation.
iii) Safeguarding Policy: MAG is committed to safeguarding the health, wellbeing and human rights of all staff, partners, and beneficiaries, and to providing a safe and trusted environment for anyone who comes into contact with our work. The Safeguarding Policy, sets out our approach and refers to a suite of policies, procedures, and guidelines in place to ensure all individuals who are involved with, or affected by our work come to no harm, distress, abuse and neglect caused by MAG. This Policy was reviewed in March 2021 and the associated policies are:
    a) Reporting Malpractice and Raising Concerns (Whistleblowing) Policy: encourages employees and others who come into contact with our work who have serious concerns to voice those concerns. MAG is committed to ensuring that genuinely held concerns will be thoroughly investigated and those who raise them will be protected against victimisation and discrimination.
    b) Policy on Personal Conduct: sets out the expectations that MAG has of all employees (including trustees, consultants, volunteers) as well as providing examples of behaviours and actions that will always be unacceptable. This policy also creates an obligation to report any concerns about the behaviour of other staff members. All new staff are required to sign to say they understand the Policy on Personal Conduct.
    c) Protection of Children and Vulnerable Adults Policy. This policy recognises that all MAG representatives have a duty of care to protect children and vulnerable adults from harm. Any form of abuse towards children or vulnerable adults by MAG representatives or other parties will not be tolerated. We have measures in place to prevent and minimise the risk of abuse, protect staff and safeguard the reputation of the organisation. This policy creates a strict obligation on all staff to report any concerns they may have which involve children and/or vulnerable adults.
    d) Dignity at Work Policy: all staff should be free to carry out their work with dignity and respect in an environment that is free from discrimination, intimidation, harassment, and bullying. In this policy, MAG sets out that it will take a zero-tolerance approach to any behaviours, which compromise these basic rights.
iv) Procurement Policy: MAG is committed to ensuring that all procurement activities adhere to the principles of value for money, transparency, and fair and open competition. We will not trade with any suppliers, which we have good reason to believe exploit people. Our procurement policy is clear Page 3 of 4 that suppliers must comply with local laws and regulations and that all procurement activities are in accordance with MAG's Ethical Statement and Financial Misconduct and Crime Policy.
v) Ethical Statement Part I: The Statement sets out our minimum ethical expectations of clients, suppliers, investors, companies, organisational and individual donors. We ensure reasonable due diligence steps to satisfy ourselves that each partnership complies with our Ethical Statement.

5. Due diligence processes

i) MAG's Background Checks Policy: sets out the checks required for all new employees, trustees, volunteers and consultants, before they engage with MAG. Key elements of this relate to modern slavery and include: Reference checks, Criminal record checks, Identity and right to work checks
ii) MAG's Partnership Policy: This policy sets out our due diligence process to ensure that MAG does not enter into partnerships with organisations with a vision, purpose or mission that are at odds with our own. The due diligence MAG carries out checks to ensure partner organisations and key partner staff are not included on any US or EU list of individuals and organisations involved in supporting or financing terrorist activities or being involved in international crimes.
iii) Vendor Due Diligence Process: MAG performs a vetting process to ensure that suppliers are not included in any US or EU list of individuals and organisations involved in supporting or financing

terrorist activities or being involved in international crimes. MAG has a proportional approach in managing suppliers' related risk, for which the level of vetting performed is directly proportional to the overall expected financial volume being potentially engaged and / or the level of potential risk related to the type of goods and services being sourced.

6. Training on modern slavery and trafficking

All new staff undergo an induction programme when they join MAG. This includes a briefing on the key policies that are listed above and training on MAG's other policies, procedures and processes including the Modern Slavery Statement. MAG runs refresher training each year for all staff on safeguarding and in local languages. Training is also conducted on effective and safe recruitment practises.

7. Our Commitment

This statement is made pursuant to section 54(1) of the Modern Slavery Act 2015 and constitutes MAG's slavery and human trafficking statement for the financial year ending 31st December 2022. It has been approved by our trustees, who will review and update it annually.

MAG 24 01 Insurance Services – Relevant MAG Policies

DATA PROTECTION POLICY (last approved January 2021)

Introduction

Data Protection Laws

This Policy reflects the requirements of the EU General Data Protection Regulation 2016/679 ('GDPR'), the UK Data Protection Act 2018 including its applied GDPR provisions ('DPA 2018'), the UK Privacy of Electronic Communications Regulations 2003 (known as 'PECR' and alternatively 'e-Privacy'), and all relevant EU and UK data protection legislation (collectively referred to herein as 'Data Protection Laws'). This Policy may be amended in response to further guidance that may issue once the UK leaves the European Union (e.g., enactment to replace the EU GDPR with a UK GDPR).

Data Protection Laws relate to any information from which an Individual can be identified (directly or indirectly) either on its own or together with other information. The DPA 2018 increased the level of potential fines for non-compliance depending on the nature of the breach, to the greater of GBP 17 million or 4% of global annual turnover.

Our donors and our regulators expect us take information security very seriously

MAG takes information security very seriously and protecting our information and IT systems is a key component of building and maintaining trust. The consequences of not securing information could expose the organisation and our brand to significant legal and regulatory censure, sanctions and fines. Personal information is legally protected and requires specific attention. Our regulators expect us to comply with best industry practice when securing all types of information.

This policy applies to everyone in the organisation who accesses or otherwise handles Personal Data

This policy applies to all Personal Data processed by MAG and is part of MAG's overall programme and approach to compliance with Data Protection Laws. This policy applies to all Personal Data processed by or on behalf of MAG (including where MAG outsources the management or Processing of Personal Data to third parties or other MAG Organisations).

All MAG Personnel (which for the purposes of this Policy includes all MAG employees, trustees, contractors and associates working for or on behalf of MAG) are expected to understand their responsibilities described in this Policy.

Non-compliance and associated data privacy risks must be identified and managed

Compliance with this Policy is mandatory. Failure to comply will not only put MAG's data protection compliance at risk, but could have disciplinary consequences for any MAG employees, associates or contractors found to be in breach, including adverse risk metrics and/or investigation and disciplinary action pursuant to the MAG Disciplinary Procedure, up to and including dismissal. In addition, breaches of Data Protection Laws can give rise to criminal and/or civil liability for the individuals concerned.

Monitoring and policy enforcement

The MAG Data Protection Lead (DPL) is tasked with monitoring the organisation's compliance with this Policy. This Policy (together with all Related Policies) is an internal document and cannot be shared with third parties, donors or regulators without prior authorization from the DPL.

Subject to applicable law or regulation, MAG reserves the right to:

- monitor, review and examine the use of MAG managed IT and information assets
- monitor and remove any software, files or information stored on any MAG managed device
- rescind access, without notice, to MAG networks and the use of MAG IT assets and resources
- discipline any MAG personnel for breaches of laws, regulation or policy

Contact us

For further information, email dataprotectionteam@maginternational.org if you would like to know more or need help with implementing this policy.

Policy ownership and approval

The Data Protection & Privacy Policy is owned by the Director of Governance and Business Transformation. This is version 0.3 and was approved by the Board of Trustees on 29th January 2021.

Definitions

- Consent – is the means by which a Data Subject signifies their agreement to the Processing of Personal Data relating to them. Consent must be freely given, specific, informed and an unambiguous indication of the Data Subject's wishes, and must be expressed by a statement or clear positive action.
- Data Controller – means a natural (living) or legal person, public authority, agency or other body which, alone or together with others, determines the purposes and means of the Processing of Personal Data.
- Data Processor – means a natural (living) or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
- Data Subject –means any identified or identifiable natural (living) person. A Data Subject is not a company or other legal person. This Policy may use the term 'Individual' as an alternative to the term 'Data Subject'.
- EEA – means the European Economic Area, which is comprised of the 28 countries in the European Union, together with Iceland, Norway and the principality of Liechtenstein.
- MAG Personnel – means employees, contractors and associates of MAG.
- MAG – we, our, us means 'Mines Advisory Group'.
- Individual – means 'Data Subject'.
- Personal Data – means any information from which, alone or together with other information, an Individual can be identified. Personal Data can be factual, such as names, identification numbers, location information, and one or more identifiers such as IP addresses or cookies. Personal Data can also be an opinion about an Individual's actions or behaviour, or related to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of an Individual. Personal Data includes 'Sensitive Personal Data'.
- Processing or Process – means any activity, operation or set of operations that is performed on Personal Data, including collecting, holding, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making available, aligning, combining, restricting, erasing or destroying.
- Sensitive Personal Data – means Personal Data that relates to an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation, as well as criminal offences or convictions. Sensitive Personal Data is referred to as Special Categories of Personal Data in the EU General Data Protection Regulation.

MAG Requirements for Handling Personal Data

In our role as a charity and an employer, MAG takes data protection very seriously, whether the Personal Data relates to our donors, suppliers, contractors, business associates or current, past, or prospective MAG personnel.

In all cases, we expect MAG Personnel and all third parties Processing Personal Data for us or on our behalf to comply with these data protection principles:

Lawfulness, Fairness, and Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner.
We will provide Individuals with clear and relevant information about how we process their Personal Data in order to ensure that the processing meets the requirements of Data Protection Laws.
Data Protection Laws permit processing of Personal Data for specific purposes to ensure data is processed fairly and does not adversely affect the Individual.

MAG must only process Personal Data when it is necessary and meets at least one of these six lawful bases for Processing:

- Consent – where the Individual has given their Consent for their Personal Data to be processed. Any processing must be strictly within the purposes for which the Consent is given. Explicit Consent is required in most cases when processing Sensitive Personal Data.
- Contract – where the processing is necessary for the performance of a contract with the Individual. This includes the performance of contracts to which the Individual is party or in order to take steps at the request of the Individual prior to entering into a contract.
- Legal Obligation – where the processing is necessary to comply with legal obligations to which we are subject.
- Vital Interests –where the processing is necessary to protect the vital interests of the Individual or another natural person.
- Public Interests – where the processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in us. (Public interests must be 'substantial' when we are processing Sensitive Personal Data).
- Legitimate Interests – where the processing is necessary for our (or a third party's) legitimate interests provided they do not override the interests and fundamental rights of the Individual. Where we rely on this lawful basis, we may need to perform a legitimate interest assessment (see 'Privacy Risk Assessments below).

Purpose Limitation

We collect and process Personal Data for specified, explicit and legitimate purposes. We will not process Personal Data in a manner that is incompatible with the originally stated purposes.
Secondary use of personal data will be reviewed and approved by the Data Privacy Office, the DPL or authorised delegate.

Accuracy

We will ensure the Personal Data we process is accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure Personal Data is accurate, having regard to the purposes for which it is processed.

Security and Confidentiality

We will take reasonable precautions to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access. These precautions include technical, physical and organisational security measures to prevent unauthorised access, as documented in the Related Policies. More information can be found in the Information Security Policy.

Data Subject Rights

Individuals' Rights. Individuals have the following rights when it comes to the processing of their Personal Data:

- Withdraw their previously given consent at any time
- Request access to their Personal Data
- Object to our processing of their Personal Data for direct marketing purposes
- Request erasure of their Personal Data if it is no longer necessary for the
- Purposes for which it was collected or required to be retained for legal and regulatory purposes
- Request rectification of inaccurate or incomplete Personal Data
- Challenge our processing of their Personal Data where we are exercising our legitimate interests

Responding to Data Subject Rights Requests.

Where MAG is the Data Controller (determining the means and purpose of processing the Personal Data), we will ensure that we comply with the following requirements:

- Information – we will ensure Individuals are informed about our privacy policies and their rights in relation to their Personal Data at the point of collection, in easily accessible notices. This includes

Personal Data collected on paper, website registration forms, surveys, and telephone and email marketing campaigns.

- Request Forms – we will provide reasonable and accessible means for Individuals to submit their requests by emailing us using the contact information within the Privacy Policy that is available on the MAG website. MAG Personnel must be able to quickly identify a DSAR, which does not have to take any specific form and can be submitted by any method.
- Safeguards – we will confirm the identity of any Individual submitting a DSAR before providing a response.
- Response – within 30 days of validating the identity of any Individual submitting DSAR, we will provide the requested information, or provide legitimate reasons for not complying with their request. In certain limited circumstances, we may need to extend our response time by up to 60 days.

Sensitive Personal Data

In providing our services, we would not usually expect to process sensitive personal data, however, we are likely to process sensitive MAG personnel information, and therefore, we will take additional measures, including applying the MAG Highly Confidential classification and safeguarding it in accordance with Related Policies. Likewise, additional measures should be applied when we are required to process sensitive personal data of MAG personnel. Where MAG acts as an independent Data Controller, we require written notification before donors disclose sensitive personal data to us.

Personal Data used for Marketing Purposes

Our marketing activities will comply with Data Protection Laws. The following direct marketing obligations will apply:

- ePrivacy. At the time we collect an Individual's Personal Data for current or future direct marketing purposes using electronic communications (fax, text, recorded telephone messages, and email), we will obtain an affirmative indication of agreement (opt-in) from that Individual to receive further marketing communications from us. A pre-checked opt-in box (requiring an Individual to opt out) will invalidate the Consent and will be non-compliant.
- GDPR. All invitations for Consent (opt-in) will be clearly written, and easy to find at the point of collection. It will be made clear at the point of collection that Consent can be withdrawn at any time, as well as the effects of withdrawal (including options for opting back in). Relying on legitimate interests for direct marketing profiling is permitted if that fact is disclosed at the time of collection, and it is made clear to the Individual that they can object to such profiling at any time.

GDPR Consent.

We will ensure that we can demonstrate:

- when the Individual has consented to the Processing (including the Purposes and Rights described at the time of the collection);
- that Consent was freely given (i.e. that the performance of a - contract or services was not conditioned on the Consent being given); and
- when Consent was withdrawn (if applicable)

Automated Processing of Personal Data

Where we process Personal Data on a purely automated basis, Individuals have the right to object at any time to our processing of the Personal Data concerning them if it produces legal effects concerning them or similarly significantly affects them. We will handle such objections through the DSR procedures outlined above.

Data Minimisation Personal

Data will be adequate, relevant and limited to what is necessary in connection with the purpose(s) for which it is processed. If we receive personal data during the course of a donor engagement which is excessive, we will endeavour to apply data minimisation by deleting the information that is not required; or returning the information to the donor and requesting a clean copy.

Storage Limitation
Personal Data will be maintained in a form identifying or rendering the Individual identifiable only for so long as it serves the purpose(s) for which it was initially collected or subsequently authorised, except to the extent permitted or required by applicable law.

Information Transfer and Compliance
We may transfer Personal Data to MAG Organisations and/or third parties on our behalf outside the UK, including to countries outside the EU or the EEA for legitimate business activities in accordance with Data Protection Laws.

Assurances.
We will not transfer Personal Data to another country or organisation outside the UK/EU/EEA unless we are satisfied that the Personal Data is adequately protected in accordance with Data Protection Laws, this Policy and our Related Policies. MAG Personnel will ensure that any such transfer of Personal Data is governed by written agreements with third parties that impose obligations that reflect the requirements of Data Protection Laws and this Policy.

If there are no UK 'adequacy regulations' about the country, territory or sector for an information transfer, it should be determined if MAG can make the transfer subject to 'appropriate safeguards'. There is a list of appropriate safeguards in the UK GDPR, such as:

- A legally binding and enforceable instrument between public authorities or bodies
- UK Binding corporate rules ("UK BCRs")
- Standard contractual clauses (SCCs)

Privacy by Design and by Default; Pseudonymisation
We are required to implement Privacy by Design and Privacy by Default by ensuring we have appropriate technical and organisation measures (such as pseudonymisation) to ensure compliance with Data Protection Laws at the outset.

- Privacy by Design. This concept promotes the identification and mitigation of privacy risks at the time a product or service is designed, so that privacy and compliance with Data Protection Laws are applied at the earliest stages of a project involving Personal Data and data protection issues are identified and addressed in advance.
- Privacy by Default. This concept ensures that, by default, Personal Data is safeguarded to the greatest extent possible. MAG will ensure that it processes such Personal Data as necessary for specific purposes of the processing, for the shortest period of time possible and with the most appropriate access controls in place.
- Pseudonymisation and Anonymisation of Personal Data. Data Protection Laws apply to information from which an Individual can be identified. Pseudonymisation and anonymisation are methods by which elements of Personal Data are removed or separated so that they cannot be linked back to an Individual without additional information. These processes require the implementation of technical and organisational measures to mitigate the risks of reversal and re-identification, where applicable.

Privacy Risk Assessments
We will assess potential Personal Data privacy risks when personal data is being processed through a change in existing process or development of a new process and or application, and apply appropriate mitigation steps depending on the outcome(s) of established processes, beginning with an analysis and applicable assessments outlined herein.

- Privacy Threshold Analysis (PTA). Answering basic questions regarding the processing of Personal Data will become an element of approving a new supplier, process, system or service. Where Personal Data is being processed, a Data Protection Impact Assessment must be completed.
- Data Protection Impact Assessment (DPIA). Completing the DPIA allows us to evaluate how Personal Data will be collected and processed, whether adequate safeguarding measures are in place, and how and when Individuals will be informed. Identified privacy risks will be evaluated and consideration given to how those risks can be mitigated in compliance with Data Protection Laws and this policy.

Where high residual risks remain, the DPL will determine what additional steps are necessary to mitigate the privacy risks identified, including reframing or abandoning the project. A record will be kept of all DPIAs, which will be periodically reviewed and updated with the process or business owners.

- Legitimate Interests Assessment (LIA). Performing LIAs are necessary in circumstances where Personal Data is being processed using the legitimate interest legal basis. The LIA will be carried out and decisions documented to evidence the balancing of legitimate interests and ensure they do not override the rights and freedoms of the Individual.

Reporting a Personal Data Breach
MAG Personnel who suspect or become aware of a Personal Data breach will immediately contact IT and the DPL at DataProtectionTeam@maginternational.org.

MAG employees will not attempt to investigate the incident, or contact any relevant donor, until they have reported the matter and have been contacted by the DPL or IT for help.
Where the incident is confirmed to include Personal Data, the DPL or authorised delegate will assist the Investigations Team, monitor and review the incident response process and provide advice regarding any donor communication.

The Data Protection Laws may require data controllers to notify a Personal Data Breach to the appropriate data protection authority and, in certain circumstances, the affected individual. Where appropriate, the DPL or authorized delegate in consultation with the Chief Risk Officer (CRO) will inform the appropriate data protection authority and, if necessary, affected individuals within the statutory notification period (within 72 hours of becoming aware of a breach involving Personal Data.).

MAG as Data Controller and Data Processor
MAG as Data Controller
MAG will act as Data Controller in relation to the processing of all MAG personnel Personal Data.
MAG is a Data Controller in most of its donor engagements. This position is supported by guidance issued by the Information Commissioner. In this context we are likely to be co-controllers alongside our donor, also a Data Controller. We will not be joint controllers, which has a specific meaning in Data Protection Laws.

MAG as Data Processor
MAG will only act as a Data Processor where we process Personal Data on behalf of the donor or other relevant party (where they are the Data Controller) and there is little or no discretion as to how the Personal Data is processed by MAG. Where we consider we are a Data Processor, we will act in accordance with the instructions of the Data Controller of the Personal Data.

As Data Processor, MAG will have a duty to help the controller comply with its own obligations under the Data Protection Laws, and the engagement terms will reflect this.

Records of Processing Activities
MAG has created and will maintain a register of all Personal Data Processing activities in accordance with our record-keeping obligations under Data Protection Laws. The tool used to register our records of processing activities (whether automated or manual) will be maintained by the DPL. The completeness and accuracy of the information recorded in the register of processing activities will be the responsibility of the heads within each business function.

When we are a Data Processor, we will cooperate with controllers' requests for sight of the register relating to our Processing of their data subject's personal data, subject to confidentiality and other legal and regulatory considerations. Relevant sections of the register must be available to relevant data protection authorities upon request.

Training and Awareness
MAG will issue mandatory annual data protection training and periodic privacy awareness communications to MAG Personnel and contractors. Records of training attendance will be maintained and monitored. Non-

completion of this mandatory training will be a breach of this Policy. All MAG Personnel are expected to regularly review the systems and processes under their control to ensure their ongoing compliance with this Policy.

Data Protection Governance

The DPL is responsible for implementing and maintaining a data privacy management programme to ensure the Processing of Personal Data meets the requirements outlined in this Policy.

The DPL for MAG is responsible for the following:

- Informing and advising MAG Personnel of their obligations under the Data Protection Laws.
- Providing appropriate data protection training to all MAG employees on the Data Protection Laws and their obligations under this Policy, and ensuring a record of training attendance is retained.
- Providing advice on Data Protection Impact Assessments (DPIAs) and monitoring their performance.
- Cooperating with relevant data protection authorities. –
- Acting as contact point for the data protection authorities on issues relating to the Processing of Personal Data by MAG, and consulting with them on any other matter where appropriate.
- Keeping the risks associated with the Processing of Personal Data by MAG under review, having regard to the nature, scope context and purposes of its Processing activities.
- Conducting regular audits and compliance reviews to assess compliance with Data Protection Laws and this Policy, along with Related Policies where they relate to the processing of Personal Data.