OPM DUTY OF CARE POLICY

1. OPM Staff

OPM is fully responsible for the security of its own staff. In this document “staff” means all OPM employees including OPM employees based in branch offices, employees of OPM subsidiary companies, Directors and Non-Executive Directors of OPM companies.

2. Suppliers to OPM with own Duty of Care

Under our client contracts OPM may have contractual responsibility for the Duty of Care for its suppliers and partners. Under OPM’s subcontracts, if the supplier is competent to take responsibility for its own Duty of Care then OPM will devolve this responsibility to the supplier/third party under the terms of our contract.

3. Partners and suppliers where OPM has Duty of Care

OPM also accepts the Duty of Care for persons such as consultants contracting in their own name as individuals or through a company where they are the only employee and, occasionally, where OPM deems that a supplier is not able to put sufficient Duty of Care arrangements in place OPM may accept Duty of Care for that supplier and its staff on a case by case basis.

Where OPM is the lead organisation, OPM may accept responsibility for security and Duty of Care of partner agencies and third-party contractors under the provisions of an agreed Services Contract. Partner agencies will need to consider the binding obligations of the Service Contract and formally acknowledge compliance. Partner agencies may receive the full support and resources of OPM as detailed in this document.

All individuals or entities for whom OPM accepts Duty of Care (including Staff) are called **OPM Personnel** in this document.

Accepting a Duty of Care, means that in practice OPM will undertake all that is reasonably possible to ensure compliance with relevant health and safety legislation, and will endeavour to ensure the provision of appropriate security measures, information and training and ensure that appropriate emergency procedures are in place.

OPM’S RESPONSIBILITIES

OPM’s Duty of Care responsibilities include:

- implement personnel procedures to clarify responsibility and prepare OPM Personnel to cope with security issues in their work, support them during their travel, and address post-travel issues.
- establish an effective incident reporting process.

- provide clear policy instructions and information to all OPM Personnel travellers to help mitigate risk.
- provide training on OPM security policy and procedures, and heighten OPM Personnel awareness.
- ensure that appropriate insurance coverage is provided or in place for all OPM Personnel travellers.
- ensure that individual wellness is included in support strategies (e.g. counselling available).
- provide access to security resources and plans, particularly for high and extreme risk areas.
- maintain crisis management plans to be used by the organisation in such an event.
- work with local/national partners, where possible, to provide briefings on security.
- collaborate with other organisations to improve security policies, practices and resources.

Responsibilities of OPM Personnel

All OPM Personnel, are obliged to follow the OPM Security Policy, all other relevant policies and procedures and all measures that have been put in place and to comply with any request relating to security made by or on behalf of OPM. This includes but is not limited to reading and understanding the travel advice issued before travel and raising any questions with the Global Security Manager (**GSM**), obtaining a Travel Authority in advance of travel, completing and updating the travel tracker and reporting any incident promptly to the GSM or the Critical Incident Management Team. Any queries or feedback (including suggestions for improvement or grievances) regarding Duty of Care should be directed to the Director of Business Services.

All OPM Personnel are also responsible for their own safety and security, and that of their colleagues. Every OPM Personnel has a duty to minimise the risks to themselves, their colleagues and OPM's property and reputation by developing their safety and security awareness and putting this into practice daily.

All OPM Personnel must:

- be responsible. You are accountable for your personal and professional actions. It is essential that you understand how your actions or inaction could put at risk your own safety and that of your colleagues.
- follow the rules. OPM's safety and security policies and procedures are in place to protect you and your colleagues, and so must be adhered to and respected. Always make sure you are aware of and comply with the travel procedures, driving rules, movement restrictions and any curfews in place.
- be cautious. Don't take unnecessary risks. No programme activity or property is worth your life. If you have concerns about your safety and security, you must raise these with your line manager, the GSM or the Country Director.
- act appropriately. Never engage in conduct that puts yourself or others at risk, or could discredit OPM or our clients and partners. Always be respectful of the colleagues and communities you are working with. If you are aware of behaviour or actions by other OPM Personnel that either breach OPM's policies or compromise team safety and

security in any way, you have an obligation to inform your line manager and / or the Country Director and the GSM.
- be prepared. Make an effort to understand and appreciate the environment in which you are living and working. Ensure that you are fully aware of the dangers that exist, you understand how to minimise the risks, and you know what to do in an emergency.
- keep others informed. Ensure your colleagues/line managers are informed of your location and movements. If you witness, or are informed of, incidents or events that affect the security or safety situation in your location you must report these to the GSM and / or the Country Director.

RISK MANAGEMENT FRAMEWORK

Protective Security Requirements:

The OPM Protective Security Requirements (**PSR**) are graduated security management requirements aligned with the Security Risk Analysis (**SRA**) of a particular context. The SRA Ratings will inform the level of response required to be compliant with PSR.

Risk Ratings:

The 5 level risk rating system is designed as country, or macro, level risk rating. However, varying levels of insecurity may exist within a country or operational area at any one time. Not all the factors listed will be present in each context; the most relevant/predominant should be used to determine the overall risk rating.

Country Risk Rating	Description
Green	Negligible Risk & Normal Operations
Yellow	Low Risk & Precaution
Orange	Medium Risk & Restriction of Movement

Red	High Risk & Temporary Relocation
Black	Critical Risk & Evacuation

- **Negligible and Low** Risk countries/operational areas work with the GSM to ensure appropriate and minimal security plans are in place.
- **Medium and High** risk countries/operational areas work with the GSM to determine implementation priorities. PSC inputs are required.
- **Critical Risk** Countries implement a full compliance checklist in conjunction with the GSM and Spearfish prior to mobilization of assets and staff.
- OPM activity in **Critical Risk** locations are approved by the MD.
- In operational areas that experience spikes in security related incidents a higher level of compliance is planned for to allow rapid implementation of more stringent security measures.

Risk Level	Comments	Measures
Negligible	Travel implemented via the TA process, travellers should be mindful of their surroundings and remain aware.	Traveller guidance notes, country risk briefing notes, project risk assessment and security regulations, standard operating procedures and contingency plans, insurance, emergency support
Low	Travel implemented via the TA process, travellers should be mindful of their surroundings and remain aware.	Traveller guidance notes, country risk briefing notes, project risk assessment and security regulations, standard operating procedures and contingency plans, insurance, emergency support
Medium	Extra oversight is applied through the TA process, but has minimal impact on travel and projects.	As above, plus trained drivers and approved vehicles, security cleared accommodation.
High	Highest level of oversight is applied. Specific security measures are implemented and actively managed for the duration of field the mission.	High risk locations directly assessed by GSM and Spearfish.
Critical	Critical risk operations approved by OPM MD.	Critical risk locations approved by MD. High and Critical Risk Travel Approval (HCRTA) countersigned by GSM. HEAT training, pre-trip briefing, measures such as close protection

		officers, satellite communications and tracking as required.

Travel

The Travel Approval (**TA**) form applies to ALL Medium, Low and Negligible risk destinations and is designed to identify when and where the individual is travelling, contact details in-country, trip itinerary, and logistical arrangements. The traveller signs the form to confirm they fully understand the risks and are willing to travel, before it is passed for management review and approval from an approved position holder for travel to commence.

In the case of High and Critical risk locations, the High and Critical Risk Travel Authority (**HCRTA**) form details the security precautions to be taken, and is counter signed by the OPM GSM and/or Spearfish SSA. Critical Risk locations require additional authorisation by the MD.

Security Resources and Support

OPM have in-house support mechanisms and resources to provide travellers with extensive security support, as detailed below. We assess the risks for each project on a case by case basis to determine whether additional external security support is required, such as close protection officers or approved vehicles.

Information

a. Quantitative Security Risk Analysis
b. Bespoke Security Regulations, Contingency Plans and SOP
c. Pre-Embarkation brief.
d. In-Country briefing via OPM staff or external agent.
e. Regular communication on changes to SRA, incidents, travel management and security plan.
f. Access to alert systems through contracted PSC.

Training

a. Security induction for new staff
b. Security Risk Management Training
c. Critical Incident Management Training
d. Hostile Environment Awareness Training (HEAT)
e. First aid training provided as required

Equipment

a. Satellite phones for redundant communications
b. Personal first aid kits
c. Grab bags provided to those who complete HEAT training
d. Electronic tracking, vehicle and personal

Support

a. Comprehensive travel insurance for staff and approved third parties
b. Medical Evacuation
c. Critical Incident Management Team and
d. 24hr emergency phone line

Security plans

Based on the findings of each SRA, a security plan will be managed by OPM staff in countries where OPM has representation via a Country or Project office and by a Private Security Company (**PSC**) where OPM is not represented by a Country or Project Office.

Independent security advisors

OPM has contracted the services of three Private Security Company's to assist in the development and management of appropriate risk management plans:

I. OPM has contracted Spearfish, a specialist provider of bespoke security services, to provide support in the planning and implementation of risk management plans

II. OPM has contracted Protection Group International (PGI) to provide electronic security information and alert systems accessible to all OPM staff.

III. OPM has contracted Terra Firma to provide bespoke Kidnap and Ransom support.

Critical Incident Management

OPM have developed a robust Critical Incident Management Protocol (CIM-P), a dedicated Critical Incident Management Team (CIMT) and a graduated Critical Incident Management Training schedule to ensure effective response to incidents in our operational areas. In the event of a Critical Incident, the CIMT are trained and equipped to coordinate a response, drawing on support networks and dedicated agencies.