Duty of Care Policy[1]

Foreword

RUSI accepts full responsibility for the security and duty of care of our staff when they travel on RUSI business, (where 'staff' includes employees and subcontractors engaged on contracts) and takes these obligations very seriously. RUSI's Director General has overall responsibility for the security of RUSI staff and assets and oversees the risk management system. This is routinely devolved to individual team directors on a day-to-day basis.

Understanding Risks to Staff, and Effective Duty of Care Plans

For RUSI staff in our offices in London, Brussels and Nairobi, or working virtually in other locations, our normal health & safety rules apply. Should international deployments be required, RUSI has many years of experience in sending staff to work in fragile and conflict-affected states. Whenever staff are required to work in high-risk destinations, a thorough Project Risk Assessment (PRA) must be carried out as a starting point for exercising RUSI's duty of care.

The PRA is designed to identify risks attached to each activity carried out as part of the project, to help in understanding those risks and deciding on appropriate mitigations. In completing the PRA, RUSI staff may make use of the Institute's networks including key government agencies, and the security industry, e.g., Healix, and Control Risks. RUSI receives live security feeds through in-country security networks, amongst others its Nairobi Office, as well as through other NGOs operating in similar environments. RUSI also engages with the British Embassy or High Commission in country to remain alert to changes in the security environment, especially while work is taking place, so that staff can be extracted.

There are a range of mitigations that may be deployed where risks are identified. These may include changes to travel plans, such as avoiding certain regions, modifying planned activities, changing modes of transport, employing the services of a security firm in country, security briefings, and recommendations on attitudes and behaviour, dress codes, general conduct, personal security awareness, additional training and so on.

The PRA must be prepared by the Lead Researcher, reviewed and signed off by the director responsible for the project.

[1] This policy does not form part of any employee's contract of employment, and it may be amended at any time.

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

Travel Risk Assessment

All RUSI staff intending to travel to hostile, or potentially hostile, territories are required to complete a Travel Risk Assessment (TRA) questionnaire before the trip can be approved. In fact, a Travel Risk Assessment (TRA) should always be completed for any business travel that is outside Europe but should also be completed for travel within Europe wherever there is a concern. The purpose of this questionnaire is to document the risk assessment procedure and explain how the risks identified will be mitigated. Before the trip can take place the traveller(s), the director responsible for the project, and RUSI's Chief Financial Officer (or in their absence another member of the Senior Management Team), must sign off the TRA. In some cases, the TRA may be escalated to the Director General and/or trustees before it is approved, and there have been instances where the proposed travel has not been signed off and has not taken place, because, on completion of the questionnaire, the risk to staff is assessed to be too high. The TRA covers the following themes: crime, terrorism, conflict/political, kidnap, government, infrastructure, as well as natural and cultural risks (profile of the traveller/customs/dress/religion etc.). The full proposed itinerary must also be recorded on the form.

Monitoring risk to Staff on an On-going Basis

Whilst staff are on a mission, we continue to monitor the security situation and any developments through the means described above, particularly by keeping a close watch on any FCDO advice and keeping in touch with our principle security risk advisers, Healix. Staff are asked to activate the Healix Travel app on their phones, and through that app have access to global incident monitoring and alerts, plus emergency assistance. Considering the countries' degree of risk and the answers provided in the questionnaire, we would require staff on a mission to check in with a designated staff member in London, Nairobi, or Brussels (usually the Line Manager) once a day at a pre-determined time to confirm that they are safe and that no security issues have arisen. All security incidents, including all near misses, must be reported to the Line Manager, and then passed on to the Director of Human Resources in London. Each incident is analysed and leads to consideration of whether procedures need to be adjusted.

Our links and relationships with local partners and associates in conflict-affected areas enable intelligence and risk assessments to be developed, fine-tuned, and crosschecked before and during deployment. Post deployment, and following unexpected or threatening incidences, senior personnel debrief those involved and look out for any signs of latent trauma, providing access to professional psychological support wherever required (With the assistance of HR).

Systems to Manage an Emergency or Incident

Staffmust book all travel and hotels through RUSI's approved travel agent. This allows RUSI staff in London and Brussels always to know the whereabouts of travellers. On the rare occasions where it is not possible to use RUSI's approved travel agent, a full and detailed itinerary must be provided on the TRA. RUSI Nairobi staff should always ensure that the Director RUSI Nairobi has their itinerary when they travel for business. Staff working in or travelling to high-risk countries may be asked to complete e-learning training modules

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org

provided by Healix and to attend country-specific cultural and security risk training including Hostile Environment Awareness Trainings (HEAT), or similar, where appropriate.

Certifications are kept up-to-date and renewed as required. Should an emergency arise, all staff are covered under RUSI's personal accident and travel insurance policy, which covers medical support including, where necessary, evacuation. In addition, travellers to high-risk territories are asked to complete a Personal Data Profile (PDP) form before they travel, and that form is lodged with the Director of Human Resources in London. It includes contact details for next of kin, blood group, details of pre-existing medical conditions, and other important details.

Extending our duty of care package to protect subcontractors

RUSI accepts full responsibility for the security and duty of care of staff while working, and the definition of "staff" includes subcontractors when they are engaged on RUSI projects. There are the following clarifications:

Subcontractors already in-country

In cases where subcontractors face risks when they already operate in a country or countries, and the individuals concerned are not travelling away from their homes or normal place of business, the assumption is that the subcontractor is already aware of the risks of the country in which he or she lives and works and has responded appropriately to ensure their safety. There is no need for a PRA, and RUSI does not take responsibility in these circumstances. Where an additional level of risk is identified, specific to the project in which the subcontractor is engaged with RUSI, then RUSI accepts responsibility for that additional risk and will work with the subcontractors to ensure that mitigations are in place.

Individual subcontractors vs organisations

Whilst both individual subcontractors and individuals working for organisations subcontracted by RUSI are covered by RUSI's travel and personal accident insurance when they travel on RUSI business, for wider duty of care purposes, RUSI draws a distinction between individual subcontractors and organisations who may be subcontractors. Whereas individual subcontractors will follow RUSI's policies, with respect to training, profiling, etc. For organisations, RUSI will work with organisations with whom it subcontracts and exercises its duty of care in respect of individuals working for those organisations by ensuring that the organisation provides suitable security provisions and policies. In some circumstances, RUSI may make recommendations that security arrangements are upgraded or improved, before the organisation can become involved in the project e.g., it may be recommended that the individuals undergo additional training.

For more information and advice on travelling with RUSI read Procedures for Staff Travelling Overseas.

The Royal United Services Institute
61 Whitehall, London
SW1A 2ET
United Kingdom

+44 (0)207 747 2600
enquiries@rusi.org
rusi.org
@RUSI_org