1.1.4 (1.4)	**Duty of Care**. The implementer will hold the duty of care responsibility for project staff, project security and, where applicable, individuals who input into/appear in project communication products.	**Pages: 2**	**Points:** 75

Duty of Care and Safeguarding. Torchlight fully understands and accepts the Duty of Care and Safeguarding responsibilities it bears for employees, subcontractors, agents and third parties affected by our activities. These obligations are taken seriously and with 7 years' experience, including the *safe delivery of over 18,000 days in Fragile and Conflict Affected States (FCAS) and complex environments such as Lebanon, Pakistan, Afghanistan and Iraq,* we have developed clear processes and procedures to ensure we address these responsibilities effectively. We have layered proactive initiatives including: formal and dynamic risk assessment and mitigation; detailed property and site security plans; secure and effective communications; working in close partnership with the Authority and all stakeholders; appropriately assessing and equipping staff; providing appropriate and ongoing training / briefings; and continually honing, testing and enforcing our comprehensive Company Operating Procedures, which keep management of risk as a central tenet throughout. Torchlight has developed a series of ISO 31000 and PAS 3001 compliant procedures which are all underpinned by Torchlight's ISO 9001:2015 certified management processes and procedures to govern our obligations.

Local/Regional Risk Factors. Lebanon presents a diverse security environment with various security issues including terrorism, cross-border conflict, crime and political instability. Terrorism currently poses more of an incidental than a direct risk to foreigners, with most attacks targeting personnel and facilities associated with the Shi'a Muslim movement Hezbollah, Shi'a civilian areas and occasionally politicians. There is a low, but credible risk of attacks targeting Westerners, primarily from Syria-based Islamist extremist groups, most prominently Islamic State or 'Daesh' and the AQ affiliate Hay'at Tahrir al-Sham (HTS). Palestinian refugees represent an estimated 10% of the population of Lebanon. Around 53% of the Palestinian refugees in Lebanon (around 450,000) live in the 12 recognised refugee camps. The ongoing conflict in Syria has forced many Palestinian refugees from that country to flee to Lebanon in search of safety. Most Palestinian militancy in Lebanon is confined to these camps.

Islamist context within Palestinian Refugee Camps (PRCs). The Palestinian Islamist scene in Lebanon is multifaceted, with a number of extremist groups operating within PRCs such as *Asbat al-Ansar*, *Jund al-Sham*, and *Fateh al-Islam*. There are a few, well-known, cases in which Salafist armed groups from camps have carried out cross-border attacks, or attacks on the Lebanese Armed Forces (LAF) and Internal Security Forces, which were coordinated with external armed groups such as Jabhat al-Nusra (now HTS). However, Salafi Takfiri Jihadist ideology has not traditionally been a driving force in the conflict in Palestine which, despite a surge in Salafi Islamism over the past eight years, has been largely secular. Nevertheless, Daesh has long-deployed narratives which use the treatment of Palestinians and the crisis in Palestine to manipulate supporters towards the terror group. Following the organisation's initial declaration of its so-called Caliphate, its leader, Abu Bakr al-Baghdadi, listed the countries where Muslims were under attack who could expect Daesh's support – this included Palestine. Daesh has also released materials directed specifically at the 'People of Palestine' in which it urges all Palestinians to be assured that Daesh is fighting in their interests and supports their 'jihad'. Torchlight maintains strong connections into LAF Intelligence – who are officially mandated to administer and police the camps – through our own ongoing security programmes in Lebanon, as well as through the local NGOs with which we are partnering on this project, which operate in all 12 of the PRCs and have excellent relationships with both the LAF and the various militias that have a presence in the camps and have existing access permits in place. We also maintain strong networks within the international NGO community, including with Field Security Officers at UNRWA. While in the camps, we will ensure our project team are accompanied by local NGO staff who are familiar with the camp, its people and protocols, at all times. We are acutely aware of the potential threats of violent backlash towards beneficiaries as a result of perceptions around this programme, and have appropriately mitigated these in the design as described Sections 1.2.1 and 1.5.1.

Cyber Threat. The cyber threat constitutes the second greatest risk, either in the form of a targeted operation by state actors, extremist or criminal groups, or indirectly because of malware infected software/hardware, which is prevalent in Lebanon. In this case, since there is a clearly defined threat and likelihood of cyber-attack, as well as the need to share sensitive personal and operational data across international borders we will ensure that a robust Information Security Management System is employed and fully understood and utilised by our project staff and implementing partners. Education, training and continued vigilance remain the best methods of reducing this risk. ***Value Add****: As a leading cyber resilience partner to governments and organisations across the globe, Torchlight will provide cyber security training to all project staff and implementing partners in the safe use and maintenance of IT, communications and social media platforms* prior to and during the project lifecycle through **CybSafe™**, our proprietary, **GCHQ- and IISP-accredited** eLearning platform. In addition to engagement with the Authority, we will constantly monitor alternative risk management sources for emerging technical threats to help inform and influence project activity.

Competent Staff and Effective Procedures Leading to a Realistic Duty of Care Plan. Torchlight has an operational team with in excess of 190 years of experience from a range of relevant public and private sector backgrounds. These individuals are suitably qualified and experienced in assessing and implementing appropriately informed, contextualised and effective Duty of Care and Safeguarding planning, risk identification and management. This experience has been used to develop exhaustive Standard Operating Procedures (SOPs), tailored to the specific environments we operate in, including Lebanon. These SOPs form the framework for our Duty of Care Plan whose core elements include: Operational Instructions, Communications Strategies, Medical Evacuation Plans, Critical Incident Management Plans, Evacuation Plans, Insurance Cover, Mandated Training (SAFE and SAFE Plus). As part of our continuous improvement model, these plans are regularly updated and are signed off at Torchlight Group Board Level, where Duty of Care and Safeguarding oversight is owned.

Risk Matrix						
Impact	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		likelihood				

Key	
	Low Risk
	Moderate Risk
	High Risk
	Extreme Risk

Understanding and Managing Risks to Staff, People and Projects. We identify, monitor, assess and manage risk continuously, drawing on multiple sources of contemporaneous and historical information, including; FCO guidance and alerts, our own in-country networks, local partners and suppliers, regional managers, corporate experience, in-house analysts and professional risk management consultancy services. This consolidated approach ensures that Torchlight's bespoke plans and security strategies are informed by a comprehensive suite of relevant policies, contexts and information feeds, and that contextually appropriate and responsive contingency plans can be implemented in a timely and effective manner. In developing our risk assessment, we include factors that could have an impact on the safety and well-being of our personnel and sub-contractors, project stakeholders and beneficiaries, as well as those that could impact our successful project delivery. We consider policy, political, security, infrastructure and environmental factors. Following best practice, we prioritise risk in terms of the multiple of the 1-5 scored likelihood and impact it could have on our dependants and the project. We mitigate where appropriate, and formally monitor indicators of a risk being manifested, and manage them accordingly, as illustrated in the table, left.

Monitoring Risk to Our Staff. As part of our continuous management of risk, projects and performance we implement a process of monitoring our staff, commensurate with our risk management plan. This includes:

- Daily communications – especially for lone workers, and those in areas of risk;
- Regular communications – daily / weekly for teams;
- Regular video or physical meetings – to confirm wellbeing of team and identify any risk that has gone unnoticed;
- 24-hour hotline – Torchlight maintain a manned emergency phone which can be contacted 24/7.
- Should the situation dictate, we have the facility to implement 24/7 GPS-based tracking of personnel through our Crisis Management partner Northcott Global Solutions Ltd – NGS - (http://www.northcottglobalsolutions.com/tracking).

A Collaborative Approach – Extending our Duty of Care to Include our Supply Chain. As we design and implement projects, we take responsibility for all personnel working on and for our projects, and adopt an open, transparent, and shared approach to both the planning and delivery of all activities. This includes the early sharing and collaborative agreement of Security Plans such that all participants understand the risks and contingent plans. We collaboratively review and refine these plans and reassess as necessary. If not already provided by subcontractors for their own staff, then we will extend our insurance policies to cover all aspects of the project and personnel. This could include K&R insurance for high risk countries, as necessary.

Assurances to HMG. Torchlight adheres to a proactive strategy that engages a full range of stakeholders, continually evaluating the threats and their potential impact on risks in light of programme outputs. In addition to our formal monthly project-specific reviews, our log frame, Risk Matrix (see Section 1.5.1) and work plan will be continually reviewed throughout the project by our Programme Manager, to highlight any risks, opportunities or significant changes, enabling us to maintain situational awareness, keep staff fully informed and adjust security measures accordingly. These will be regularly communicated to HMG project managers using a RAG security dashboard. We will report on all project staff who undergo our pre-deployment Hostile Environment Awareness Training (HEAT). Using Threat/Risk monitoring, newsfeeds and local information, we will monitor the security situation and liaise with the Authority and End User clients regarding threats/risks on route, on-site and in the vicinity of project focused sites. We encourage observation or participation by HMG project managers as a further means of re-assurance

- **Email Security.** As part of Torchlight's normal business, we manage the passage, storage and management of sensitive data through Switch Secure Email and File Transfer. Egress Switch is a UK-based software company and is recognised by CESG's Commercial Product Assurance for sharing data at OFFICIAL-SENSITIVE. This resource can be managed on all devices, including IOS, Android and regular PCs and Apples, and utilises FIPS 140-2 encryption. Data can also be shared with one-time users for free with tokens that are sent with the secure email thus providing a versatile and effective secure communication system.
- **Secure Document Management.** Further to effectively managing the security of emails, we also use Switch Secure Workspace. This is also a secure application produced by Egress and assured by CESG for Availability, Confidentiality and Integrity of the project information. It allows the secure production, management and sharing of project documents up to SECRET. We will manage the access control and administrative rights to this web space and be able to set up and remove users as they are required to use the space, as well as set up secure and shared work spaces with other stakeholders for short- or medium-term duration as the project dictates. Movement and onward dissemination of any information is also strictly controlled.
- **Cyber Security Awareness Training.** We will ensure all personnel with access to project communication devices are trained and made aware of the Cyber security threat and how to manage it. This will include using **CybSafe**, our internationally recognised, GCHQ-accredited web-based Cyber Awareness Training tool. Torchlight developed this online tool which will be employed to inform and train the users in ensuring data is stored, shared and managed correctly; how to recognise cyber threats and attacks; how to respond and report on them; and how to manage personal and physical security of their devices.
- **IT Security.** All Torchlight devices are protected by Microsoft's BitLocker disk encryption. This is a fully supported mechanism of locking down hard drives at rest, maintaining the confidentiality of the device if it is mislaid, lost or stolen. In addition to this, mobile devices are managed with Meraki Mobile Device Management, which allows us to centrally manage company mobile devices across the globe, enforcing security policies, deploying software and applications safely, live troubleshooting and remote data wipes of devices if lost or compromised.