HRM03: Global Safety & Security Policy 2021

1. Purpose

The purpose of this policy is to ensure that TLM staff and representatives are safe and secure while working for TLM. The safety of our people is TLM's primary priority, above the security of property, assets, or cost savings. TLM, however, accepts there is a certain amount of risk involved in fulfilling our mandate and we are committed to ensuring that steps are taken to minimise these risks. This is not only a legal requirement, but also our moral duty. We need to provide a safe working environment for our people, in order to fulfil our mission and vision.

To articulate our strategic approach to Safety and Security, and to aid the management of risks to within limits that we consider to be acceptable, TLM has developed this global safety and security policy and the accompanying procedures. These were created bearing in mind the variety of places where we operate and the nature of our work.

The Global Safety and Security Policy and Procedures apply to Implementing and Supporting countries. All TLM entities (Members, Affiliates, TLM International and TLM Trading are expected to:

- Adopt the minimum standards of the global safety and security policy
- Contextualise the global safety and security procedures.

2. Definitions

For the purposes of the safety and security policy and procedures:

- **"TLM Staff"** includes all TLM employees, working part-time or full-time.
- **"TLM Representatives"** includes for example: TLM volunteers, interns, Board members, consultants, visitors, and all who officially represent TLM in any way.
- **"TLM Affiliate"** refers to countries that are not currently Members of the Global Fellowship but want closer interaction with and support from The Leprosy Mission.
- **Safety** refers to accidental risks (e.g., car accidents), physical and mental health risks (e.g., sickness or post traumatic disorders) and natural risks (e.g., flooding).
- **Security** refers to the potential and actual effect of violence (e.g., conflict, assault, abduction, and criminality).
- **A 'critical incident'** is one that because of its severity (see section 12) or the sensitivity of the situation may result in, or has the reasonably foreseeable potential to result in, harm to person(s), operations and or the reputation of the organisation.

3. Duty of Care & Responsibilities

TLM has a legal and moral duty of care on safety and security for staff and representatives. TLM will take all possible and reasonable measures to reduce the risk of harm to those working for TLM. Although prevention is our main approach, we recognise that we cannot create a risk-free environment where incidents will never occur. TLM's duty of care will respond to any incident or critical incident that may occur by the following supporting mechanisms:

- **The Global Fellowship Board** has responsibility for ensuring that a global policy, such as this, is in place and is regularly reviewed.
- **The Local Board** is responsible for ensuring that local country-level safety and security policy and Procedures are in place (based on TLM's global policy and Procedures) and

are regularly reviewed. Where appropriate, local Boards are encouraged to appoint a Trustee responsible for Safety and Security.

- **Country Leaders:**
  - Are ultimately responsible for ensuring safety and security in their country. They may choose to delegate certain responsibilities to specific members of staff.
  - Will need to develop and implement their own local country safety and security policy and procedures, based on this global policy and procedures.
  - Must ensure that all staff and representatives receive regular and appropriate training.
  - In the event of a security incident, will be responsible for co-ordinating all internal and external communications, including media activity. In some cases, this will require consultation with TLM International.
- **Local Security Lead**: Members are encouraged to appoint one or more Local Security Leads depending on the size and spread of the country operations. This will normally be a staff member, but in some cases may be a Board member. The Local Security Lead should not be the Country Leader but should support the Country Leader in promoting staff safety and security, and in implementing the appropriate policies and procedures.
- **All TLM staff and representatives:**
  - Must accept individual responsibility for their personal security as well as the security of their colleagues, programme activities, and the organization. Staff and representatives must seek to minimize risks by following preventive procedures that are in place.
  - Must understand and comply with this policy before undertaking international travel on behalf of TLM.
  - Are expected to behave in accordance with TLM policies and procedures, and in a manner that does not place them, their colleagues, or our clients at any undue or unnecessary risk.
  - Must ensure that they have adequate means of communication and are contactable at all times. To ensure this TLM should check connectivity coverage in areas of our activity and should make available the provision of local reliable SIM cards when necessary. Work communication costs can be recovered by staff or representatives as appropriate.
  - Must report any security incidents or 'near misses' as soon as possible to the Country Leader or Local Security Lead.

4. Risk Appetite

Although Members of the Global Fellowship make many autonomous decisions, TLM's underlying **Risk Appetite** is defined as follows:

Staff and representatives are the most important assets to TLM. Each TLM Member commits to putting measures in place to minimise and manage risks to people and will make operational decisions based on such assessments. At times this will mean not operating in certain regions, or at certain high-risk times. In some cases, it may mean we need to cancel or postpone activities and programmes; or review the safety and security procedures in order to better manage risks. TLM will not expose staff and / or representatives to work in environments where the likelihood and the impact of potential harm is high.

TLM recognises and acknowledges that perceptions of risk can be variable and subject to biases, meaning that whatever risks we are able to tolerate as an organisation may not always align with what individuals feel comfortable in accepting, therefore TLM will always listen and consider individual preferences before making decisions.

5. TLM's Safety and Security Principles

a. **TLM values life over property.** Staff and representatives must not put their lives or the lives of others at risk in order to achieve project aims or to protect TLM or another organisation's property.

b. **TLM values all staff and representatives equally** and while specific provision may be made for different groups of people, this does not indicate different levels of value. TLM recognises that different groups may face different levels of risk in different societies (e.g., due to gender, ethnicity, religion) and if necessary, TLM will make specific provision for those that face particular risks as a result. In some cases, TLM may not be able to deploy staff of a particular group in a particular area.

c. TLM staff and representatives must, in general, be prepared to travel to and work in areas with some level of safety and security risk. However, TLM staff and representatives have a right to refuse to travel to locations or undertake any activities on TLM's behalf that exceeds their own personal risk thresholds.

d. TLM will never compromise security standards due to lack of funding. Where sufficient funds are not available to ensure the minimum standards of security, TLM will not commence or continue programme activity.

e. TLM staff and representatives must respect any decision made by TLM to postpone travel, or to withdraw staff and representatives from a location due to safety and security concerns. If staff or representatives act against a TLM decision to withdraw from a location, TLM may no longer be able to take responsibility for their security and this may be considered a disciplinary issue.

f. TLM's goal will always be the safe release of hostages (detained or kidnapped staff and representatives). However, TLM will not pay ransom in any circumstances, believing that the payment of ransom builds the capability of terrorist groups and finances their activities, while also increasing the risks to TLM and other organisations by encouraging further hostage attempts. TLM will request all parties involved in critical incident management, including ransom and release negotiations, to adopt the same stance.

g. TLM takes safety and security very seriously and any deliberate violation of this Policy may lead to disciplinary action being taken.

6. TLM's approach to Security

Security must be actively managed, not just planned for, and is most effective when fully integrated into organisational management (programmes, people, finances etc).

a. **TLM's primary approach is to mitigate risk by acceptance.** Acceptance means building a safe operating environment through consent, approval and cooperation from individuals, communities, and local authorities.

b. **TLM's secondary approach is protection.** This involves reducing the vulnerability of TLM to a possible threat, for example, by hiring guards or using CCTV. Improving safety and security practice through risk assessment and mitigation is also a protective measure however, "hard protective measures" (e.g., armed guards, armoured vehicles) are not suitable at TLM (unless under specific circumstances and with pre-approval from the International Director). We prefer to seek a safe environment for our activities than to be forced to run our operations by using hard protective measures.

c. **Deterrence aims to reduce risk by discouraging, minimising, or preventing the threat**, for example temporary suspension of programme activities. This approach is generally to be considered as a last resort, used under high-risk situations.

In addition, TLM recognises the role that our Christian faith, including but not limited to prayer and spiritual insight, plays in ensuring the safety and security of our staff and representatives. Therefore, prayer is a key component of TLM's response and prevention mechanisms, and prayer support will be raised whenever required.

7. Relationship with other organisations

a. **Partners:** TLM's partners are responsible for managing their own security. When visiting or working alongside partners, TLM staff and representatives must ensure that the security procedures agreed with the partners are appropriate and sufficient, and that they align with TLM policy and procedures.

b. **Security networks:** TLM recognises and supports a collective security approach within the NGO community. Where possible, Members are encouraged to join or be in contact with local security networks such as that of other NGOs and the United Nations. Within the bounds of confidentiality and staff security, TLM will cooperate closely with other organisations in order to best manage security. At the discretion of each Member, this may include information sharing, joint training, and pooled resources.

c. **Armed security & use of weapons:** TLM will not use armed protection e.g., armed guards or armed escorts. This is because it contradicts TLM's approach and is fraught with potentially negative consequences. TLM will not permit armed personnel (security forces, military, police, or guards) to travel in/with TLM vehicles. An exception may be made under specific circumstances and with pre-approval from the International Director.

8. Security Planning

Security Risk Assessment

Each TLM Member (and Affiliate) should carry out regular safety and security risk assessments (LINK) for each location in which it works. The risk assessment and mitigation steps should reflect the risks to all staff and representatives, including any cross-cultural staff or visitors (international or national).

Security Rating

The overall safety and security risks shall be allocated a **security rating (as standard TLM uses Green, Yellow, Orange, and Red - see Procedures section 3 - LINK)** and the security ratings shall be communicated in local security Procedures. Each TLM Member (and Affiliate) should regularly review their security rating. Further information about TLM's security ratings can be found in the TLM Safety and Security Procedures (link).

9. Security Briefings & Debriefings

Each Member is responsible for ensuring appropriate and timely security briefings and debriefings are conducted for all staff and representatives. This includes before, during, and after national and international travel. Such briefings and debriefings should be appropriate according to the length and scope of the trip and its security risks. Members must ensure staff and representatives are fully briefed on the risks of any TLM trip and have understood and agreed the mitigation measures in place to minimise the risk.

10. Induction, Training & Equipment

TLM will take actions to build the safety and security awareness and capacity of its staff and representatives. Country Leaders will ensure that staff and representatives have access to training as appropriate to their job responsibilities, the level of risk, and local context. For all positions (including short assignments), a general safety and security briefing should be included at induction.

TLM has an obligation to provide appropriate equipment to ensure staff and representatives can safely carry out their work.

11. Incident Management

A security 'incident' is any event, circumstance or significant context change that affects the security of TLM's staff or representatives, assets, or operations.

All security incidents, including minor incidents and near misses, must be reported immediately to the Country Leader or Local Security Lead. Critical incidents must also be reported to the International Director.

Incident reporting & analysis is crucial for follow up to the specific event, as well as informing organisational learning. A review should always be carried out after an incident (or near-miss) to ensure steps are taken to prevent it from happening again. When appropriate, security reports will be shared with others to aid their awareness and learning (e.g., United Nations, other NGOs, local authorities, etc).

In the event of a security incident, the Country Leader will be responsible for co-ordinating all internal and external communications, including media activity. In some cases, this will require consultation with TLM International.

12. Critical Incident Management

A 'critical incident' is any event that seriously threatens the welfare of staff or representatives or result in death or life-threatening injury or illness. A critical incident may also involve TLM clients, or anyone TLM comes in contact with, when they are harmed or threatened as a consequence of TLM actions. In the case of a critical incident, TLM's priority is to secure all staff and representatives safely without putting others at risk.

In safety and security incidents involving sexual harassment and / or assault, the Safeguarding Team will be informed, and a coordinated response will be implemented in line with the critical incident management procedures and safeguarding policies.

13. Insurance & Support

As part of its duty of care, each TLM Member should ensure that their staff and representatives have appropriate work-related accident, and travel insurance.

In case of any incident, TLM will respond quickly, compassionately and provide support including medical care, psychosocial, emotional and prayer support to individuals, as appropriate, and as is reasonable and possible in each circumstance.

14. Revisions

This Global policy will be reviewed every 2 years to ensure compliance as well as ensuring lessons learnt are incorporated.

Each Member will review their contextualised local policy and procedures at least every two years. A range of local staff should be included in the review process as much as possible.

All policies and procedures may be updated more frequently if external or internal circumstances change to ensure high standards of practice.

Related Documents

Safety and Security Procedures
Strategic Human Resources Framework
Safeguarding Policy
Safeguarding Procedures
Bullying and Harassment
Disciplinary guidelines
Whistleblowing Policy

Policy versions and updates

Changes made	Version	Date	Review and Approval
Created	V1	2008	Created by HR Manager Approved by Board
Reviewed – no substantive changes made.	V2	December 2014	Reviewed by Head of Human Resources Approved by Board
Comprehensive review and restructure Added: Page 1 – additional definitions Added: Section 3 - Duty of Care and Responsibilities Added section 4 - Risk Appetite Reviewed and expanded: Section 5 - S&S principles Added: section 6 – TLM's approach to security Added: section 6 –Relationship with other organisations Added: section 9 – Security Briefings and Debriefings Added: section 10 – Induction, Training and Equipment Added: section 11 – Incident Management Added: section 12 – Critical Incident Management Added: section 13 - Insurance and Support	V3		Reviewed by Head of People