TRANSPARENCY INTERNATIONAL RWANDA

Security Policy

February 2025

Contents

1. Principles on Safety and Security

The safety and security of our staff and field teams are a key responsibility of our organisation. We accept a duty of care for all staff and field teams. With an increasing number of travels to several (post)conflict countries, we are committed to a clear, relevant and proportional TI-Rwanda security policy, protocols and plans.

The aim of the policy is to increase the security awareness of all staff and field teams involved so as to create a culture of security, and ultimately, to enable the travels that our work requires.

The key to effective safety and security management is the creation of a culture of security and TI-Rwanda will work to create such an environment. Each staff and field team member has a responsibility for their own safety and security and that of others. Furthermore, we belief each staff and field team member has a duty to address issues of safety and security – proactively and frankly – at all times.

A definition for safety and security is difficult to pinpoint. As a general definition we apply the following: The state of being protected against (external) threats and the condition of being safe; free from risk or injury.

2. Security strategy

TI-Rwanda is a nongovernmental organisation (NGO). As such it adopts the principles of non-partiality and neutrality that steer the thinking of the majority of organisations in the non-profit world. This is a strategy that TI-Rwanda considers most appropriate.

The acceptance strategy can, dependent on the level of risk in a country, be combined with protective measures. We avoid deterrence measures as much as possible. Even though protection measures may be necessary, the centre of gravity rests with an acceptance approach. TI-Rwanda and its representing staff will avoid the use of armed protection.

3. Design and Implementation of the Security Policy

The security policy is developed by the TI-Rwanda management, in concurrence with all TI-Rwanda staff. The policy will be reviewed and updated on a yearly basis and when changes in circumstances affecting TI-Rwanda in any way require it. Feedback and suggestions for changes to the policy should be forwarded to the Programme Manager.

Review and implementation of the policy lie with the TI-Rwanda's Programme Manager, who is held accountable by the TI-Rwanda's Executive Director. The authority to enforce implementation of the policy rests with the TI-Rwanda's Programme Manager.

4. Roles and Responsibilities

Every individual at every level has specific roles and responsibilities. This chapter outlines at which level certain responsibilities lie and where staff or field team members should look for guidance or action concerning safety and security issues.

4.1 Headquarters Level

Programme Manager
- Thoroughly reading, accepting and complying with the TI-Rwanda Security Policy and Security plan
- Setting the security policy and protocols for the organisation
- Producing security plans for the field missions, which can then be adapted to each different field context
- Training policy
- Providing competent field teams
- Planning of field operations
- Allocating sufficient resources, both financial and human
- Providing support to field teams when necessary
- Monitoring the effectiveness of security management in the field

- Ensuring lessons are learned from experience and that policy and procedures are updated accordingly
- Taking appropriate corrective action to address deficiencies in security procedures

Executive Director

- Thoroughly reading, accepting and complying with the TI-Rwanda Security Policy and TI-Rwanda Security Plan
- Deciding on deployment or evacuation
- Ensuring that designated staff at the Headquarters is well prepared to take timely security related decisions when necessary. This includes the preparedness and implementation of a crisis management team for managing certain serious or high-profile incidents
- Being aware of the extent of legal liability if various contingencies were to occur
- Taking appropriate corrective action to address deficiencies in security procedures

4.2 Field Level

Team member

- Thoroughly reading, accepting and complying with the TI-Rwanda Security Policy, TI-Rwanda Security Plan and SOPs
- Participating actively and proactively in security assessments during the field operation
- Contributing actively to developing the rules for the trip and committing to active participation in the establishment of these
- Taking appropriate corrective action to address deficiencies in security procedures
- Acknowledging the authority of the TI-Rwanda team leader in security and behavioural aspects

Team leader

- Thoroughly reading, accepting and complying with the TI-Rwanda Security Policy, TI-Rwanda Security Plan and SOPs
- Guiding of and taking responsibility for all TI-Rwanda team members, under delegated authority of TI-Rwanda

- Taking local responsibility for implementation of security measures and behavioural aspects
- Taking responsibility for field operations, including TI-Rwanda money and assets, under delegated authority of TI-Rwanda.
- Assessing the security situation during the field operation
- Reviewing and completing the field security plan delivered by TI-Rwanda.
- Reviewing and completing the SOPs delivered by TI-Rwanda.
- Staying in contact with TI-Rwanda Headquarters.
- Deciding on evacuation
- Taking appropriate corrective action to address deficiencies in security procedures

4.3 Personal Level

Operating with security awareness in order to assure in the best possible way the safety and security of team members, the field team and the organisation at all times, in every level of the organisation.

5. Extent of the Security Policy and protocols

All TI-Rwanda staff and all individuals contracted by TI-Rwanda on a professional or voluntary basis working on a TI-Rwanda activity are covered under this policy. The policy does not cover family members of the above individuals and staff under contract with other NGOs or institutions. People are the organisation's highest priority. The policy only covers people, not material and financial assets. It provides guidelines on the physical workplace security, cyber security and health security.

6. Guidelines on physical workplace, cyber and health security

6.1. Physical workplace security

6.1.1. Secure the front desk

TI-Rwanda's front desk is one of its first lines of defense. TI-Rwanda makes sure it is armed with the tools it needs to keep it secured against bad actors. A visitor management system is established to help create a more secure and cohesive workplace. Beyond security, a visitor management system solution offers insights into space usage and occupancy trends. This can come in handy when designing the lobby layout and finding potential security gaps.

6.1.2. Offer unique WiFi credentials for visitors

TI-Rwanda wants every visitor to feel welcome and safe when they walk into its building, and that includes giving them automatic WiFi access. However, TI-Rwanda assign unique access codes to visitors to avoid potential security threats, like hacking or cyberattacks.

6.1.3. Monitor who is onsite at all times

TI-Rwanda wants to make sure those coming in and out of the building are supposed to be there. TI-Rwanda established a simple way to track employee and visitor registrations. It is especially crucial during an emergency, when first responders and safety teams know who is onsite, they can guide everyone to safety more effectively.

6.1.4. Install a badgeless access system for employees

Badge entry systems are not as secure as you may think. With the right tools and wrong intentions, anyone can clone a badge and use it to enter a workplace. Luckily, modern technology has come a long way in creating an easier solution. TI-Rwanda installs access control software to keep its workplace secure while making it convenient for its team (who may have forgotten their badges).

6.1.5. Use a password protection tool

Every employee uses several platforms and apps to get through their day's work. Keeping track of all those passwords is not only a headache but also a workplace security concern. TI-Rwanda considers investing in a single sign-on tool that secures a number of login credentials under one main password. This will help keep the employees' passwords secure in one place and limit the possibility of hacks.

6.1.6. An emergency notification system

Every organization needs a fast and reliable way to keep employees and visitors safe and accounted for during emergencies. TI-Rwanda installs systems that send real-time alerts through SMS, email, and push notifications so that everyone gets the critical information they need, no matter where they are onsite. To stay prepared, TI-Rwanda keeps contact information for all onsite personnel up to date so no one misses an important emergency alert.

6.1.7. Provide security training and resources to employees

Employees often make mistakes that may seem harmless, like letting unauthorized guests in. But, these "harmless" mistakes can actually open opportunities for bad actors. TI-Rwanda makes sure to arm the employees and other personnel with helpful tips to stay protected. Additionally, it is a must for employees and other personnel to know where emergency exits and first aid kids are kept and they can help employees and visitors better navigate the workplace during emergencies.

6.2. Cyber security

According to Rwanda Investigation Bureau (RIB), the rate of cybercrimes increased by 72% during the first COVID-related lockdown[1]. At TI-Rwanda, security teams must dedicate significant time to protect our work from hackers, phishing, insider attacks, and more.

---

[1] Emmanuel Côme Mugisha, "Cybercrimes increased by 70 % during lockdown –RIB", The New Times (2020): https://www.newtimes.co.rw/article/178791/News/cybercrimes-increased-by-70-during-lockdown-a-rib, accessed on 30/12/2024.

Some measures should be taken to protect us against any breach of our organization's critical company data. This includes:

- Data stored across devices, networks, and the cloud.
- Two-factor authentication, encryption, and backups
- Removal of access rights (termination) for all departing or resigning personnel, both employees and contractors/third parties.
- Limit unsuccessful logon attempts.
- Protect wireless access using authentication and encryption.
- Users must be given unique IDs;
- Ensure that executives, senior management, managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
- Provide security awareness training on recognizing and reporting potential indicators of insider threat.
- Conduct an awareness campaign on cybersecurity among clients and stakeholders.

6.3. Health security

TI-Rwanda considers health and safety very important when considering the overall workplace security. Every TI-Rwanda team member is obliged to make sure they have all necessary vaccinations and other medical precautionary measures.

Drugs and alcohol are not allowed in the workplace and staff are strictly prohibited from working while under the influence of drugs or alcohol. TI-Rwanda will not tolerate staff working under the influence of drugs or alcohol, and any staff member who is found to be impaired in the course of his / her employment will be subject to discipline up to and including termination of employment for just cause.

TI-Rwanda encourages its employees to do annual health checks and provide a medical certificate to TI-Rwanda Office. Furthermore, TI-Rwanda encourages all its employees to do exercises either personal or in groups such as sports organised during car free days.

7. Nature of the Security Policy

Adherence to the policy is a requirement. Only in life threatening situations team leaders have the authority to bypass these to a certain extent. Failure to adhere to the policy may lead to non-employment by TI-Rwanda in the future.

All staff and field team members covered under the policy and protocols as stipulated in section 5, have the right to decline to enter high risk environments without impacting employment. They also have the right to leave locations where their personal assessment is that their safety and security or that of others is being compromised.

When despite of the risk assessment the security situation deteriorates beyond limits of acceptability both TI-Rwanda management as well as TI-Rwanda team leader have the possibility to decide upon evacuation and this decision cannot be overruled. Both scenarios will be under full responsibility of TI-Rwanda as are the costs incurred.

If and when an individual team member within a team does no longer feel comfortable with the security situation, the team member has the right to depart earlier at his own costs and responsibility.

8. Code of Conduct

This Code of Conduct seeks to guard our standards of behaviour. It seeks to maintain the high standards of independence, effectiveness and impact to which TI-Rwanda aspires.

Respect and Care for the Participant/Client

We shall adopt a professional association with participants/clients and respect their culture, beliefs and background. We take participants seriously; "there are no stupid questions". We develop a safe learning environment, where participants/clients feel comfortable to approach us. Training courses can be overwhelming and participants can get emotional. Please take this into consideration. Controversial topics (such as abortion, faith and politics) must be treated with sensitivity.

Respect for Culture and Custom

We will endeavour to respect the culture, structures and customs of the communities and regions we are working in. As a team member of TI-Rwanda, one is automatically a representative of the organisation. The team member will act as an "ambassador" as much as he/she is a staff, trainer or consultant. At the moment the team member travels internationally for TI-RWANDA, his behaviour will be subject to close scrutiny by both the NGO staff as well as the wider public in the "host community".

TI-Rwanda and its representatives will respect the law and the culture of the host community. This implies that cultural rules concerning expected dress codes, non-use of alcohol and other restrictions are respected to a sensible degree. Before each travel the individual has the obligation to study the context and the cultural laws of the country of destination.

Continuous improvement

We want to improve constantly, maintaining and heightening the standard of our activities. TI-Rwanda's representatives shall provide feedback to TI-Rwanda and be honest about it. Complaints shall be addressed to TI-Rwanda, not to participants or clients.

9. Protocols

TI-Rwanda considers the following protocols, part of the security policy, to be binding for all individuals covered under the security policy as stated in paragraph 5.

9.1 Briefing

All TI-Rwanda representatives travelling for TI-Rwanda will be briefed before departure, either by email, in person or both. The briefing will contain logistical, content related and security details. Whenever possible and appropriate, TI-Rwanda will arrange security briefings upon arrival at the location of destination. Upon return, all TI-Rwanda representatives will fill out a mission report and can request a debriefing.

9.2 Travel – Preparation

Training

Before departure, all team members receive an appropriate safety and security training. The training course certificate has to be submitted to the TI-RWANDA office.

Health and Safety

Every TI-Rwanda team member is obliged to make sure they have all necessary vaccinations and other medical precautionary measures.

Emergency Precautionary Measures

Before travelling to a field operation, all TI-Rwanda team members must fill in a personal profile (including proof of life questions) and submit the document to the TI-RWANDA office.

Cancellation

TI-Rwanda makes the decision to cancel or continue planning the mission. However, TI-Rwanda stays responsible for continuous monitoring. If changing security situations require cancellation or evacuation, TI-Rwanda has the obligation to do so. With regard to these decisions, TI-Rwanda acknowledges the importance but non urgent nature of its mission.

9.3 Travel – Execution

Composing Standard Operating Procedures (SOPs)

Staff at all levels should continually monitor significant political, social, economic and military events in the areas where TI-Rwanda works. Often those best able to conduct assessments in a specific country or region are the field teams working within them. Therefore, team and team leader have primary responsibility for composing Standard Operating Procedures (SOPs). Writing the SOPs is not, however, a onetime event. It is a continuous process. Threats and organisational vulnerabilities can change frequently.

With each change, the risk to field teams may increase or decrease and safety and security measures should be adjusted accordingly.

9.4 Communication

Before travelling, the TI-Rwanda office and the TI-Rwanda team leader will determine the interval of the communication. In case of loss of communications longer than a certain number of hours (also to be determined beforehand) TI-Rwanda will contact the nearest embassy and report the situation. Depending on the situation, TI-Rwanda will set the crisis plan in motion.

Contact within the team will be preserved at all times. Team members must be aware of the location and communication means of their travel companions. If the team goes separate ways for whichever reason, team leader will ensure that the different parties have means of communication and will determine the interval of the communication.

Telephone

The TI-Rwanda team leader and each individual member of the TI-Rwanda field team have the obligation to be able to use a telephone.

9.5 Crisis Management

TI-Rwanda defines as a crisis any unstable situation of extreme danger or difficulty, which harmfully affects or can harmfully affect the organisation and/or its representatives.

Evacuation

When during field operations the security situation deteriorates beyond limits of acceptability, both TI-Rwanda management team (Executive Director and Programme Manager) as well as TI-Rwanda team leader have the possibility to decide upon evacuation and this decision cannot be overruled. Both scenarios will be under full responsibility of TI-Rwanda.

9.6 Incident Reporting

TI-Rwanda defines as an incident all events, which have caused, are likely to cause or could have caused the low profile of the organisation and/or its representatives to be harmed (e.g. unwanted contacts with or questioning by police, intelligence services or any other authorities).
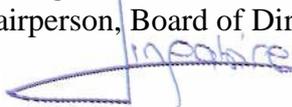
All incidents involving TI-Rwanda team members must be reported as soon as possible by all means to the TI-Rwanda office. Ultimately, a full written incident report shall be handed over by the TI-Rwanda team leader with an analysis of the sequence of events, and conclusions and recommendations (see Annex for template full incident report).

10. Evaluation and review

TI-Rwanda is committed to ensuring that this policy is a useful and current tool and therefore undertakes to carry out formal review of the policy and related documents/guidance annually. TI-Rwanda will respond to social and political situations as and when they occur ensuring that staff have the most current and valid information to inform their decisions.

This policy has been reviewed and approved during Transparency International's Board Meeting of February 10th, 2025

Mrs. Ingabire Marie Immaculée   Mr. Apollinaire Mupiganyi
Chairperson, Board of Directors   Executive Director

Annex:

Full Incident Report

Date   :
Author   :
Role of Author (involved or not)   :

Full chronological account of the incident
Who was involved?
Reasons for any decisions taken
Identification of any failure of procedures or plans, and recommendations for any actions

Signature Author:..............................