

Safety and Security Policy

Approved by: The Board of ForumCiv
Approval date: 2020-06-22
Period of validity: Until further notice
Responsible: Secretary General
Published: Intranet

Contents

| | |
|--|----|
| Safety and Security Policy | 1 |
| 1 Introduction | 4 |
| 1.1 Purpose, Scope and Limitations | 4 |
| 1.2 Compliance..... | 5 |
| 1.3 Relation to other policies, codes and guidelines | 5 |
| 1.4 Duty of Care..... | 5 |
| 1.5 Priority..... | 5 |
| 1.6 Acceptable risk | 5 |
| 1.7 Equal rights..... | 6 |
| 1.8 Do no harm..... | 6 |
| 1.9 Working with partners/Transfer of risks..... | 6 |
| 1.10 Accountability..... | 6 |
| 1.11 Transparency..... | 6 |
| 1.12 The right to withdraw..... | 7 |
| 1.13 Involvement with arms | 7 |
| 2 Organisational Commitments | 7 |
| 2.1 Standard Operating Procedures..... | 7 |
| 2.2 Incident reporting and incident management..... | 7 |
| 2.3 Contingency Plans | 8 |
| 2.4 Security Risk Analysis | 8 |
| a) Annual Contextual Risk Assessments..... | 8 |
| b) Local security risk levels | 8 |
| c) Local Safety and Security Plans..... | 8 |
| 2.5 Travel..... | 9 |
| 2.6 Collaboration and information sharing..... | 9 |
| 2.7 Information and communication security..... | 9 |
| 2.8 Visibility and external communication..... | 9 |
| 2.9 Resourcing security | 10 |
| 2.10 New programme areas..... | 10 |
| 2.11 Insurance | 10 |
| 2.12 Training..... | 10 |
| 3 Responsibilities..... | 11 |
| 3.1 Management responsibility | 11 |
| 3.2 Individual responsibility | 11 |

| | | |
|-----|---|----|
| 4 | Annexes Standard Operating Procedures and Templates | 12 |
| | Safety and Security Risk Management..... | 12 |
| | • Location Risk Rating Matrix..... | 12 |
| | • Annual Contextual Risk Assessments | 12 |
| | • Site Safety and Security Plans | 12 |
| | Travel Safety..... | 12 |
| | • Information Security Management..... | 13 |
| | • Classification of projects and information | 13 |
| | Incident Reporting and Incident Management | 13 |
| 5 | Annexes Contingency Plans..... | 13 |
| 5.1 | General note on Contingency Plans | 13 |
| | • Natural disasters | 13 |
| | • Fire emergency..... | 13 |
| | • Medical emergencies | 13 |
| | • Evacuation | 13 |
| | • Bomb threat/threatening calls..... | 13 |
| | • Suspicious mail | 13 |
| | • Active shooter | 13 |
| | • VCP/Hostile roadblocks | 13 |
| | • Sexual harassments and assault..... | 13 |
| | • Kidnap and hostage..... | 13 |
| | • Arrest and detention | 13 |
| | • Burglary, unauthorised entry and theft | 13 |
| | • Demonstrations..... | 13 |

I Introduction

ForumCiv and our partners often work in complex and demanding environments and sometimes operational activities presents threats to personnel and assets. ForumCiv has a duty of care for employees, members of the board, consultants and interns who work for or provide their services to the organisation.

Creating safe and secure working environments is critical for ForumCiv and this is done through actively and continuously assessing the risks and treating/mitigating them to the extent possible. Security must be actively managed and is most effective when fully integrated into programme management. Good safety and security risk management is a pre-condition and enabler for programme delivery. It is important that this work is done with the perspective of the safety and security of any person acting on behalf of – or in cooperation with ForumCiv. Safety in this context is defined as freedom from the risk of harm as a result of *unintentional* acts, such as natural disasters, accidents or illnesses while security is defined as freedom from risk or harm resulting from *intentional* acts.

ForumCiv is a decentralised organisation with offices in multiple countries and locations and the detailed application of ForumCiv Security Risk Management will therefore vary. However, the system as it is presented in this policy and in the attached Standard Operating Procedures will apply throughout the organisation regardless of location or contractual situation of staff or other representatives of the organisation.

To reflect both internal and external changes in the socio-political environment of our work, the scope and content of this policy will be reviewed every 2 years. This document is for internal use only and must not be shared externally without prior written consent by ForumCiv's Security Coordinator.

I.1 Purpose, Scope and Limitations

The purpose of this policy is to mitigate risks for staff, programmes, trademark and assets related to ForumCiv.

This policy:

- outlines commitments and principles of ForumCiv as an organisation in relation to safety and security
- clarifies the responsibility of staff and management respectively; and
- provides a set of mandatory Standard Operating Procedures (SOP) and Contingency Plans against which compliance can be measured (Annexed).

This policy applies to all persons employed by ForumCiv, including board members, consultants, interns, or other persons representing ForumCiv regardless type of contract, all of which hereafter referred to as 'staff'. This policy applies during working hours wherever ForumCiv staff is working and 24/7 for representatives travelling outside of their duty station or sent out on expatriate contracts. ForumCiv's security measures depend on representatives acting responsibly and strictly following all security regulations and instructions. Therefore, any representative is

expected to strive to be good representatives of ForumCiv also outside of work hours and to always follow the ForumCiv Code of Conduct.

Should staff themselves in harm's way for reasons not connected to their work with ForumCiv, there shall be no Duty of Care expected from ForumCiv.

1.2 Compliance

Compliance with the safety and security policy and standard operating procedures is mandatory for all staff. Any breach will be considered as misconduct and disciplinary measures might be taken.

1.3 Relation to other policies, codes and guidelines

- Code of Conduct
- Anti-corruption Policy
- Whistle blowing Guidelines
- Equal treatment Guidelines
- Media and Communication Guidelines

1.4 Duty of Care

ForumCiv as an employer has a legal obligation to avoid the risk of foreseeable injuries to its staff. National legislation imposes obligations on employers to ensure safety in the workplace. ForumCiv exercise its duty of care through the application of this safety and security guideline, and other management policies, guidelines and procedures as well as following the national legislation of the employment.

The duty of care covers staff who have agreed to this policy and its standard operating procedures. To ensure compliance ForumCiv must pro-actively brief staff on the risks, need for the staff to give informed consent (i.e accept the risk) and on the right to refuse activities considered by him/herself to be generating unacceptable risks.

1.5 Priority

ForumCiv always put the life of staff above its physical assets, its reputation or trademark.

1.6 Acceptable risk

While ForumCiv accepts that some risks cannot be eliminated, staff will never consciously be placed at unacceptable risk levels in order to reach programmatic or other objectives. Regular risk assessments paired with relevant risk mitigation will be part of ForumCiv's standard operating procedures covering for example planning for programmes, travels, events and local security plans.

ForumCiv seeks to reduce threat by building good relations with local communities and relevant stakeholders and thereby gaining *acceptance* and consent for the organisation's presence and work. By using specific measures (e.g. surveillance cameras, locks and standard operating procedures) ForumCiv use *protection* to safeguard its staff and locations. Should ForumCiv resort to *deterrence* it would primarily relate to halting operations, cutting financial support only in exceptional cases resort to threats or arms.

1.7 Equal rights

Staff might face differences in risks related to their gender, ethnicity, nationality, religion, sexual orientation, pregnancy, disability or health status as well as position in the organisation, country of duty station etc. ForumCiv considers the safety and security of all staff equally important and no group or individual will be valued higher than another. The measures introduced to mitigate risks are always tailored to the local context and where appropriate also to the individual risk that staff carry with them.

1.8 Do no harm

Activities that cause or are perceived as causing harm to the local population or fuel conflicts could also present an increased risk to ForumCiv's staff, operations, reputation, trademark or assets. Therefore, contextual analysis and security risk management is an integrated part of programme planning, implementation and continuation.

The "do no harm" principle is a baseline for ForumCiv in our joint work with partners in conflict areas.

1.9 Working with partners/Transfer of risks

In accordance with ForumCiv's policy platform, our way to achieve results is to work through local partners and with the local population, adopting a rights-based approach. This approach builds trust and acceptance from which we also draw our main security approach. The acceptance principles fill an important part in the risk management strategy where local understanding, acceptance and tolerance can allow employees to work safer. Strict adherence to the neutrality, impartiality and independence may increase acceptance, especially if paired with the principle of 'do no harm'. If we, and our partner organizations, are accepted and valued by the local communities, it is less likely that security incidents will occur.

In contexts where our work will not gain a wider acceptance from for example authorities the acceptance strategy will need to be combined with extra measures to protect our staff, partners and operations.

ForumCiv will always strive to ensure its actions and activities do not lead to transferred risks to partners and will regularly have dialogues with partners to ensure partner risks are not transferred to ForumCiv.

1.10 Accountability

Accountability for safety and security in ForumCiv rests with all staff as outlined under the section Responsibilities in this document. Staff will be held accountable for their actions and failure to adhere to standards may lead to disciplinary actions.

1.11 Transparency

ForumCiv strives for openness and transparency in decisions, both to staff and to partners and other stakeholders. Staff has a right to ask for the underlying reasoning for decisions in relation to security risk management. ForumCiv management will to the largest extent possible be open and forthcoming to such questions. If the transparency would put integrity or safety of staff at risk, management may choose to not share information.

1.12 The right to withdraw

ForumCiv is responsible to proactively and timely inform staff about security risks to ensure staff can give 'informed consent' (I.e accept the degree of remaining risk) and accept individual responsibility for safety and security of him/herself. Staff can always choose to not participate in activities should the risk be assessed as too high. No negative career consequences should interfere with such a decision. ForumCiv will prepare employees to manage and treat risks as well as to ensure to follow-up incidents and make post-incident care available through insurances and specialists

1.13 Involvement with arms

To avoid being associated with armed violence ForumCiv will avoid using armed guards, armed escorts and armed protection of transport or premises. There might be exceptional circumstances where armed guards are needed to protect the security of staff. These cases will be reviewed by the Security Coordinator and the operational manager while the final decision rests with the Secretary General.

2 Organisational Commitments

2.1 Standard Operating Procedures

Compliance with the ForumCiv Safety and Security Policy is ensured by a set of Standard Operating Procedures and to them attached templates. Compliance to these procedures is mandatory for all staff and deviations from these procedures can only be agreed by a senior manager in writing. The Security Coordinator should always be given a copy of this documentation.

2.2 Incident reporting and incident management

A manager's ability to understand the current situation and to adapt to changes is crucial in ensuring safety and security for the organisation. By reporting incidents, we alert ourselves to threats and vulnerabilities and help prevent and reduce safety and security risks. The *incident reporting and incident management SOP* defines when, how and by whom incidents should be reported and indicate the severity of the incident. It is always better to report too often than not at all, and it is every staff member's duty and right to report incidents using the set template. Managers have the responsibility to follow up incidents and give feed-back to the reporting staff member. The Security Coordinator monitors the system and make trend analysis on incidents to help identify key threats and vulnerabilities that ForumCiv is facing.

Any incident up to the level of serious will be handled within normal management structures.

Critical incidents will be managed following the *SOP for management of critical incidents/Critical Incident Plan* and the relevant *Contingency Plan*. In such instances normal chain of command might be replaced by Critical Incident Management Teams (CIMT) lead by the Secretary General or as otherwise delegated by her. Kidnapping, abduction, accidents with severe injuries, the death of staff or third party caused by ForumCiv staff, or the need for relocation or evacuation are examples of incidents that would be dealt with by a Critical Incident

Management Team. Staff expected to work in an incident management team shall be trained in their role regularly.

2.3 Contingency Plans

Contingency plans (CPs) give specific instructions for specific situations and are to ensure that ForumCiv's staff members know what to do when normal operations have been disrupted. ForumCiv has contingency plans for emergencies covering both natural disasters and man-made emergencies. The contingency plans are in place to give instructions and/or guidance on how to contain or minimise damage, injury to or loss of personnel or assets and minimize reputational damages and to maintain continuity of operations. It is mandatory for ForumCiv's staff to follow the instructions and advices included unless an Incident Management Team instructs differently. Contingency plans can at times and in agreement with the Security Coordinator be further developed for specific locations.

2.4 Security Risk Analysis

a) *Annual Contextual Risk Assessments*

Annual local safety and risk assessments will be done to ensure ForumCiv has a good understanding of the risks it operates. These assessments will factor in political, economic, sociological, technical, legal and environmental factors (PESTLE) but also look at for example staff access to healthcare, transportation, insurance and the relationships FS has with various actors in the area of operation. The assessments will cover both operations (programmes) and locations (offices and accommodation) and be done at least once a year.

Risk treatment will always factor in the 'do no harm' principle¹, effectiveness and costs.

It is the responsibility of the local manager to ensure compliance with the system and the Security Coordinator has a supporting and quality assuring function in the process.

b) *Local security risk levels*

Risk classification of locations where ForumCiv works or regularly travels to are used as a complement to operational and geographical risk analysis. This safety and security risk classification is set by the security coordinator and responsible managers using a combination of externally and internally available information. The ForumCiv risk classification is used to define measures and procedures for travels and local security plans. In line with the SOP on *Location Safety and Security Risk Classification*, the system is updated at least bi-annually and is driven by the security coordinator.

c) *Local Safety and Security Plans*

All ForumCiv offices shall have a Local Safety and Security Plan which spells out safety and security risks and outlines the procedures in place to mitigate them. The local safety and security plan shall be based on the contextual risk assessment and the local security risk index. It is the country managers responsibility to ensure the plan is updated annually. The Security Coordinator is supporting the process and quality assuring the results.

¹¹ The do no harm principle was developed by MaryB. Anderson. <http://conflictsensitivity.org/do-no-harm-local-capacities-for-peace-project/>

Local security plans will always be accompanied by risk treatment plans at the local level.

All staff must read and accept the procedures outlined in the Safety and Security Plan of offices they work in or visit and it is the responsibility of the local manager to ensure the local plan is made available as preparation for an assignment or visit.

2.5 Travel

ForumCiv recognises that staff and others representing the organisation are at risk when travelling. To minimise the risks ForumCiv applies mandatory travel procedures for cross-border and domestic movements. The procedures are adapted to risk levels identified in the local risk rating², the local security plans and insurance covers. For travels in or to locations assessed to be high or extreme risk additional measures are applied and the decision to green-light a trip rest with the Deputy Secretary General. There is always the possibility to consult and coordinate with the Security Coordinator.

2.6 Collaboration and information sharing

In general good relations and communication with partner organisations, other (I)NGOs or civil society actors, local authorities, local and international security forces, embassies etc is a crucial component of good safety and security risk management, particularly in the field of acceptance for our work and as feed-in to the contextual risk analysis.

ForumCiv takes the position that to actively share information and knowledge with other actors on safety and security is a means to improve the security of all. In line with the framework 'Saving Lives Together'³ ForumCiv is a member in various safety and security networks and platforms at country and regional levels. In contexts where the work we are doing or supporting does not have a wide acceptance from either authorities or the wider public, we need to take the opposite approach to openness and transparency to protect staff, partners and operations.

2.7 Information and communication security

Information related to Safety- and security trends or incidents should in principle always be shared to improve our joint awareness on risks. In incident management the integrity of staff and operations will be a guiding principle for both the sharing of information internally and externally and for the means of communication. All devices used for communications (phones, laptops) issued by ForumCiv to staff are assets of the organisation. The *SOP for management of critical incidents/Critical Incident Plan* regulate how to communicate and share information in these circumstances while the *SOP on Information Security Management* regulates how to protect ForumCiv and its partners against unauthorised access to information and good information management within the organisation and with partners in normal times.

2.8 Visibility and external communication

While ForumCiv in general aims to share its activities with full transparency there might be instances when external communication or visibility need to adapted to protect partners or ourselves. Any decision to restrict our communication on activities shall be based on a

² See Location Risk Matrix which is updated biannually or as needed.

³ <https://www.unocha.org/es/themes/saving-lives-together-slt>

programmatic or local risk assessment in line with the *SOP Safety and Security Risk Assessments* and specific guidelines for means and contents of communication shall be issued by the Security Coordinator and endorsed by Deputy Secretary General for local level and Secretary General for global level.

Public statements or other forms of communication through news or social media must be in line with *ForumCiv Guideline on Media Communication* and *SOP for management of critical incidents/Critical Incident Plan*.

2.9 Resourcing security

ForumCiv considers the cost of meeting duty of care obligations to staff to be integrated in all its activities. ForumCiv also accepts that costs for safety and security will differ depending on location, activities and persons involved. Further the resourcing for safety and security must include both hard (e.g. communication equipment, locks and cameras) and soft (e.g. developing an acceptance strategy, ensuring staff is trained) security as direct costs. The overall resourcing of safety and security rests with the Secretary General while all applications for activities and funding must include costs for safety and security into their proposals. This will be visibly seen in that there is a specific budget line for safety and security.

2.10 New programme areas

Safety and security will be a key aspect in discussions on new programme areas or locations. The responsible line-manager will together with the security coordinator make a safety and security risk assessment in line with the *SOP on Safety and Security Risk Analysis*.

2.11 Insurance

ForumCiv will ensure that all staff have insurances that meet minimum standards in the context where they work. Staff shall also have insurance covers for domestic and cross-border travels. The insurance will cover extra costs related to war and civil unrest in locations where such risks have been identified. The insurance will also cover unexpected needs for evacuation.

Consultants and other third-party on assignment for ForumCiv must be covered by a travel insurance up to the same level and any contract need to document who is to cover the expenses and assure that there is an insurance cover for the person travelling.

All persons travelling as staff of ForumCiv or on assignment by ForumCiv must document that they are aware of and accept the foreseeable risks related to the travel and that they will follow the rules and procedures.

2.12 Training

ForumCiv is obliged to ensure staff receive security training as appropriate to the roles, responsibilities and contexts that come with their jobs. The line manager is responsible to ensure adequate training is given while the Security Coordinator and HR will make an annual training plan based on needs and priorities.

Safety and Security forms part of induction training for all staff to ensure understanding of the Safety and Security Risk Management framework the ForumCiv rests its work on.

Work in or visits to locations classified as High or Extreme risk require additional training and briefings and it is the responsibility of the line-manager in cooperation with the Security Coordinator to ensure compliance as spelled out in the *Travel Safety and Security SOP*.

3 Responsibilities

3.1 Management responsibility

Security Risk Management requires clear and hierarchical lines of decision-making. For ForumCiv Security Risk Management is based on the concept of line management where the Secretary General is responsible towards the ForumCiv Board for the safety and security of staff.

Following the line-management structure of ForumCiv managers have a duty to ensure compliance with the ForumCiv security risk management framework (policy, SOPs, template). Tasks related to security risk management can be delegated to individual staff members but never the responsibility.

Acceptable risk levels for operations are set by the management of ForumCiv and this responsibility cannot be delegated. Deviations from the policy and procedures must always be discussed with the Security Coordinator and the decision to grant a deviation rests with the superior line-manager.

The Security Coordinator is responsible for the process of reviewing the safety and security policy and its standard operating procedures and templates regularly or on demand from the organisation. Together with local security focal points, the Security Coordinator is responsible for developing, disseminating and maintaining ForumCiv's security instructions and quality-assuring local security plans.

3.2 Individual responsibility

ForumCiv's security risk management rests on the notion that every individual representing ForumCiv have a duty to ensure their behaviour and actions does not have a negative effect on their own or colleagues' safety and security. It is mandatory to follow policies, procedures and local security plans and it is the responsibility of the staff member to ensure he/she keeps informed of risks to themselves, their colleagues and the organisation. Any breach will be considered as misconduct and disciplinary measures might follow.

Informed consent, i.e acceptance of the foreseeable risk in relation to travel, field missions etc, is always the individuals' responsibility to give in line with procedures. Should the risk be seen as too high by an individual staff member, he/she at all times have the right to refuse to travel or participate in activities. (see the right to withdraw)

It is mandatory to report incidents in line with the SOP for *Incident Reporting and Incident Management*.

4 Annexes Standard Operating Procedures and Templates

Safety and Security Risk Management

- *Location Risk Rating Matrix*
- *Annual Contextual Risk Assessments*
- *Site Safety and Security Plans*

Travel Safety

- *Requests for travel*

Information Security Management

- *Information Security Management*
- *Classification of projects and information*

Incident Reporting and Incident Management

5 Annexes Contingency Plans

5.1 General note on Contingency Plans

- *Natural disasters*
- *Fire emergency*
- *Medical emergencies*
- *Evacuation*
- *Bomb threat/threatening calls*
- *Suspicious mail*
- *Active shooter*
- *VCP/Hostile roadblocks*
- *Sexual harassments and assault*
- *Kidnap and hostage*
- *Arrest and detention*
- *Burglary, unauthorised entry and theft*
- *Demonstrations*