Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

H2N Conflict Sensitivity and Security Management

This H2N is based on the Directive on Security Management at the FDFA (2021) and on the Good Practices for Working in an Insecure Environment (Guidelines 2011). The purpose of this H2N is to give orientations to SDC's staff on essential elements to consider when integrating conflict sensitivity in security risk management, as well as to give the link to relevant security documents from the Crisis Management Centre (KMZ).

In fragile and conflict-affected contexts where SDC is engaged, staff members, implementing partners and beneficiaries can be exposed to high security risks that have an impact on their professional and private lives. Conflict-sensitive security risk management is a key requirement for all programmes implemented in such contexts and has to be integrated in the planning, implementation, monitoring and evaluation processes.

1. Security analysis and assessment

A sound context analysis is a necessary starting point for security risk management (Directive on Security Management at the FDFA 2021). This analysis must be conducted in an inclusive way, be regularly re-assessed and integrate perspectives of a variety of staff members, according to the following steps:

• **Analyze the context:** the CSPM Tool Box introduces key context analysis tools that structure the analysis of the context with conflict-sensitive lenses. Besides, the MERV document registers the medium-term changes and allows for an early assessment of the possible influences these changes might exert on the programmes and on personal security.
SDC Guidelines for the monitoring system of development related changes MERV

• **Understanding ourselves:** it is essential to analyze how the SDC/FDFA is perceived by other relevant stakeholders regarding image, acceptance and role; and what the relationships are between the SDC and the different implementing partners in regard to security-related aspects.

• **From 'Do No Harm' towards the prevention and transformation of conflicts:** ensure that SDC-funded programmes systematically reinforce positive effects and minimize negative effects (cf Tool "Connectors & Dividers"), while addressing structural causes of conflicts, contributing to building trust between development actors, and supporting activities that connect people across conflicting lines.

• **Understand the relationship between security threats**: assess the likelihood and consequences of the security incidents and threats and carefully consider that expat staff and local staff might have different levels of vulnerability to the same security threat (cf "Guidance on Protection").

2. Measures and responses

Based on the outcome of the analysis and assessment approach, the next step is to address the risks:

• **Develop and diversify SDC's local networks with various stakeholders, incl. the civil society organisations**, in order build trust, share relevant information and gain consent for programmes as a means to minimizing or removing security threats. Acceptance can be fostered through conflict-sensitive communication (cf "CSPM & Communication" Tool), local networking and community involvement.

• **Define protective measures, procedures and devices** that reduce the vulnerability to the specific security threats. It is essential to be conflict-sensitive while defining the appropriate measures, knowing that there are two different levels of security responsibility: on the one hand for FDFA Swiss and local staff and, on the other hand, for implementing partners, human rights defenders (Swiss Guidelines for human rights defenders), and other key partners.

3. Security monitoring and reviewing

On-going monitoring and evaluation are essential to keep track of the evolving security situation, the proper application of conflict-sensitive measures and the analysis of security incidents. It is crucial that FDFA staff is complying with the security-related procedures. The main recommendations are:

• **Ensure regular Security Monitoring** by SDC staff in charge, and through regular exchanges with other relevant development partners, in order to identify changes in security conditions. It is important to diversify the network of security monitoring partners, incl. the civil society.

• **Adaptive Management / Remote Monitoring**, especially in fragile contexts, can be the only option to staying engaged in highly difficult and volatile security situations. In the frame of its Fit-for-Fragility endeavor, SDC promotes Adaptive Management, incl. Remote monitoring.

• **Incident Analysis:** report any serious security incident, investigate and analyze it (e.g. through a security incident list) in order to help prevent future incidents, and/or mitigate their effects.

• **Compliance Monitoring:** to maintain the agreement between staff members and the organization, staff responsible for security should keep other team members constantly involved through briefings, reminders about aspects of the agreement, and by asking for people's opinions and views on how appropriate and effective the current procedures and measures are in practice.

References:

Directive on Security Management at the FDFA (2021)
Good Practices for Working in an Insecure Environment (Guidelines 2011)
SDC Guidelines for the monitoring system of development related changes MERV
SDC Adaptive Management Guidelines, incl. Remote Monitoring
Swiss Guidelines for human rights defenders

FCHR, 20 September 2021