***Training Materials on the International Protocol***

**PART IV MODULE 8 – SAFETY AND SECURITY**

**Session objectives:**

By the end of the session, participants should be in a position to:

* Recognise the necessity of developing a global security strategy
* Identify common threats to practitioners, information, victims/witnesses and others
* Develop and put in place security protocols and other measures to prevent, mitigate or respond to identified risks

**Suggested duration of session:**  90 to 180 minutes

**Exercise:** None

**Relevant sections of International Protocol:**

Pages 104-117; Module 2 – Understanding Sexual Violence; Module 7 – Do No Harm; Module 9 – Planning; Module 10 – Types of Evidence of Sexual Violence; Module 11 – Interviewing; Module 13 - Storing and Handling Information; Module 16 – Sexual Violence against Children; Module 17 – Sexual Violence against Men and Boys; Annex 2 – Conducting Threat and Risk Assessments; Annex 5 – Organisational Security Good Practices Checklist; Annex 6 – Grab Bag Content

Guidance on the overarching topic of safety and security and strategies to mitigate risks to practitioners, information, victims/witnesses and other people who may be at risk due to documentation/investigation initiatives are found throughout all modules. In addition, in view of the critical importance of this subject, this module specifically deals with safety and security issues and outlines minimum guidance to take into account. It is in particular closely linked to Module 7 (Do No Harm) and Module 9 (Planning) as all three modules cover essential and sometimes overlapping security considerations presented from slightly different angles. Module 7 sets out what threat and risk assessments are and the methodology to follow to conduct them, which is further detailed in Annex 2 (Conducting Threat and Risk Assessments), while Module 9 covers risks as one of the preliminary issues to research, assess and include in your CARSV documentation plan prior to embarking on any type of investigation or documentation exercise. As previously mentioned, the trainer for these modules should have experience in planning and managing documentation processes.

This module or elements of it should form part of any CARSV documentation training programme as evidence gathering exercises undertaken without having in place a robust security plan are usually doomed to failure and likely to cause serious harm to victims/witnesses as well as other individuals directly or indirectly involved in the documentation process, including victims’/witnesses’ family members and friends, and any intermediaries, interpreters and drivers.

It may be of great importance for the trainer to remind participants to do research on the law applicable to the security (including duty of care) dimensions of a particular documentation/investigation. In some countries, documenters’ or their organisations’ duty of care and/or other security-related legal obligations may be broader or narrower than what they think. Moreover, depending on the context, the law in issue may be the law of the country where the documentation or investigation takes place, the law of the country where the organisation undertaking the documentation or investigation is based or where information/evidence is held, and/or international law. In issue is not only the law, if any, in relation to the physical security of documenters and others involved in documentation or investigation initiatives, but also the law on the psycho-social and other responses for the benefit of victims of security incidents and the law on data security/ privacy. Failure to factor the applicable law into the design of a holistic security strategy (and otherwise as part of the overall documentation/investigation-planning process) may result in the legal liability, reputational damage and financial ruin of documenters and/or their organisations.

Throughout the module, the trainer should encourage participants to assess and discuss how they and their organisations are approaching security issues, whether the level of risk they themselves feel comfortable with is aligned with the way their respective organisations address security considerations, whether they have ever felt uncomfortable with certain practices, how to deal with conflicting views, and main areas for improvements. The trainer should emphasise that even if in many organisations security planning management is the responsibility of specialised focal points and outside of the remit of documenters, participants are ultimately responsible for and should take ownership of their own personal security as well as the security of their colleagues, victims/witnesses and others who may be at risk due to the documentation effort. This is an area where no one can afford to feel shy and where participants must be empowered to speak up should they feel uncomfortable at any point. For seasoned documenters used to operating in high risk environments, complacency can be their biggest enemy.

Throughout the session, the trainer should encourage participants to discuss their previous experience (if any) with security planning management or threat and risk assessments, or with the consequences of failing to properly assess risks to victims/witnesses, staff members, other people, or information. If the group does not have much experience of this issue in a professional context, they should be encouraged to think about how carefully they assess potential risks to themselves, their family and others. If they have ever taken out insurance, carried an umbrella or decided to lock the doors to their home, they have conducted a risk assessment whether they realised it or not. The trainer should emphasise that this issue is particularly important when investigating or documenting sexual violence as there may be unique threats or risks of harm that are specific to or more severe for victims or witnesses of sexual violence than other crimes (reprisal, rejection, imprisonment), or for practitioners and others involved in documenting sexual violence committed by police, armed forces (including militias), other state officials, and other powerful leaders (specific targeting, judicial harassment, administrative withdrawal of your license to operate, etc.).

Best practice requires measures taken by organisations to be mainstreamed across all areas (personal security, human resources, facilities and office security, programming, travel and transportation, communication and data, health and wellness) as further detailed in Annex 5 (Organisational Security Good Practices Checklist). The aim of security risk management is to mitigate identified risks and to reduce them to an acceptable level. What constitutes an acceptable level of risk may be different for different organisations or people and will constantly vary through time depending on various factors (changes in threats, the political landscape, personal circumstances, perpetrators investigated, etc.).

After slide 7, the module is split into three separate sections covering: A) risks to practitioners (slides 8-11); B) risks to information (slides 12-15); and C) risks to victims/witnesses (slides 16-19), although in reality a compartmentalisation is not possible and risk should be assessed and managed holistically. For example, risk to information due to poor communication security - such as mentioning victims’ names or other identifying information over unprotected emails or in public places - may expose victims to retaliation by perpetrators and rejection by their families as well as put the security of practitioners at risk.

Participants should first and foremost be aware of the risks to their physical and psychological health and well-being to which they may be exposed a result of their work (slides 8-11). Staff members and contractors (including drivers, intermediaries) who are investigating or documenting sexual violence as well as their families/friends may be targeted in a way that those working on other issues like socio-economic development or education might not. Participants should be encouraged to think about threats specifically relevant to them, colleagues, contractors and others who may be at risk due to the documentation effort, either because of the context or situation on which they work, a particular investigation or case, or who they are (e.g. if you are documenting sexual violence crimes allegedly committed by high-ranking state officials you may face attempts to silence you through intimidation, judicial harassment, arbitrary arrest and detention or even extrajudicial killing; if you are a sexual violence survivor who has become an activist you may be more prone to vicarious trauma and require ongoing psychological support to conduct CARSV documentation work).

Following the threat and risk assessments methodology presented in Annex 2 (Conducting Threat and Risk Assessments), the trainer should encourage participants to assess the risk or likelihood of specific threats materialising and look for *bespoke mitigating factors*. In addition, participants should be referred to Annex 5 (Organisational Security Good Practices Checklist) and consider *general organisational measures* that they/their organisations may want to consider taking to prevent or mitigate common threats and risks. The standards listed constitute a starting point for building strong safety and security management practices. Practitioners should keep in mind that they are not expected to cover all safety and security approaches and contexts and that there may be situations where it is not possible to meet these standards. The trainer should also flag to participants Annex 6 (Grab Bag Content) which contains a tentative list of items and equipment – which they should tailor to their specific needs - that participants may want to consider carrying with them at all times during field trips.

Information management and security (slides 12-15) is a critical component of overall risk management as confidentiality breaches may not only compromise the documentation process as such but also have serious adverse consequences for the personal safety of individuals. The trainer should underscore that in addition to more obvious *external* threats to information such as theft, surveillance, interception or hacking, it is important to keep in mind that threats can be *internal* as well and that they do not need to be malicious to have devastating effects. Generally speaking, our ability to identify digital threats is not as developed as our ability to identify physical threats, especially for people with limited computer literacy. The trainer must make sure that participants understand how important it is for them to get a good understanding of the software and other digital tools that they may use in their work and keep up to date with security updates of computers, phones and other mobile devices, apps and other software, and new tools and technologies.

For instance, some participants may use or consider using mobile apps or other digital tools specifically developed to securely take pictures and/or videos or otherwise document atrocities and send the encrypted data to a secure repository. Whilst such tools may have some extremely useful features, it is important that participants ask themselves questions such as: Will having such apps and encrypted data on smartphones or other devices not in itself draw unwanted attention? What happens to the content once it has been uploaded? Is the content encrypted automatically at the time of collection or only once it is uploaded? Who owns/controls the content’s future use once it has been uploaded? In which country is the server based and does this raise issues around privacy or government surveillance?

The trainer should ensure that participants think about potential threats and mitigating measures covering both data that is being communicated (information “*in-transit*”) (e.g. face-to-face, telephone, Skype or other internet-based conversations, emails, online chats, text or voice messages, information being uploaded or downloaded from a cloud storage and their meta-data) and data that is being stored (information “*at rest*”) (e.g. hard copies or USB keys containing documents left on desks, in vehicles or stored in filing cabinets, digital files saved on a hard drive, cloud storage or on digital devices and their meta-data). The trainer should encourage participants to think of possible steps that they/their organisations could take to protect information and highlight that: they may include measures at the *organisational level* (e.g. information sharing practices on a strictly need-to-know basis, information security policies covering access to sensitive information, data communication and storing, use of social media, their handling during documentation mission and transportation, training of staff on communication security and digital tools, absence of disciplinary repercussions in case of immediate disclosure of a confidentiality breach, etc.), but also *practical measure*s to protect office premises (e.g. secure doors and windows that can be locked, trained security personnel, fire-fighting equipment, shredders to safely destroy documents, etc.) and *behavioural measures* (e.g. not leaving electronic devices or sensitive information at home or in a vehicle if you are not there, never allowing people - cleaners, builders - in your home while you are not present, not discussing sensitive information with colleagues in taxis or in cafes, never posting pictures or information on social media about your current whereabouts, etc.).

The last component of the module (slides 16-19) covers the management of risks to victims and witnesses, including their families/friends and communities. Guidance and strategies in that respect are found throughout the Protocol, and covered in more detail in Module 7 (Do No Harm), Module 9 (Planning) and Module 11 (Interviewing). When discussing potential threats and risks to victims and witnesses (e.g. social stigma, divorce, family rejection, loss of marriage opportunities, loss of access to education or livelihood, re-traumatisation due to a lack of gender-sensitivity by poorly trained service providers, arrest and detention, etc.) the trainer may consider going back to some of the slides in Module 2 (Understanding Sexual Violence) on the impact of sexual violence and/or the visual on who may cause harm to victims (perpetrators, family and community, practitioners and institutions) in Module 7 (Do No Harm).

The trainer should stress that as part of documenters’ research of potential threats at the planning stage, they should consult with victims and witnesses to hear from them about individual, local and community risks, keeping in mind however that victims/witnesses may both not recognise threats or minimise the risks as a coping mechanism, or have unfounded fears due to past traumatic experience or a lack of information. The threats and risks may vary between men, women and children, and between individuals within each of these groups. Individuals may be much more concerned with ensuring their anonymity and protecting the security of their CARSV-related information than in relation to other types of crimes. The emotional and psychological consequences for the individual telling their story can be more severe with sexual violence than with some other crimes; in many contexts, this may be especially true for children and men.

The trainer should remind participants that for each identified threat, participants will need to assess the severity of the potential harm on victims/witnesses, the likelihood or risk of the threat materialising and look at possible mitigating measures. It may not always be possible to avoid all harm – some risks are unforeseeable, some individuals can be severely re-traumatised just by being reminded of what happened to them. The main message to get across is that if the conclusion of their threat and risk assessment is that a risk remains too high despite mitigating measures considered, then that witness or information should not be pursued or contact with a victim/witness postponed to a later stage.

The trainer should also remind participants that as documenters they should refrain from infantilising victims/witnesses by deciding on their behalf that they need protection. *Depending on the specifics of the situation*, and provided that they are *fully* aware of the risks to themselves (and others), the victim/witness remains the ultimate decision maker on his/her risk tolerance and documenters should give priority to the opinion of victims/witnesses and their willingness to participate in the documentation process.