tool 45 Information Management

Factsheet

In order to protect the safety and privacy of victims and to mitigate risks for the organization's information, cases of grave violations must be handled with strict respect for confidentiality rules. This implies special precautions when collecting, storing and sharing such information.

Security and confidentiality when collecting information

Assess your vulnerability to situations that may compromise your and your source's security and/or the confidentiality of information and select relevant mitigating steps according to the level of risk:

Risk	Level (high/ medium/low)	Suggestions
Information may be overheard or relayed to persons who do not *need* to know it		□ Choose an appropriate location if you are conducting interviews. □ Do not discuss case information with or in front of people who do not ***need*** to know it (e.g., taxi or office drivers, cleaners and other support staff, colleagues from other projects or organizations, personal friends, neighbors, relatives, etc.) □ Avoid communicating sensitive information by phone if there is a risk your telephone may be tapped and use extreme caution when you must do so (e.g., using code words). □ Do not leave case information in plain sight or in shared spaces. □ Do not send case information through others, unless specifically allowed to do so.
Information may be lost		□ Always keep case information with you until you can store it. □ Keep copies of case information in a safe place. □ Use codes for victim, monitor, location, violation and perpetrator.
Information may be seized (arrest, roadblock, checkpoint)		□ Use codes for case, victim, location, focal point, perpetrator. □ If there is an imminent or likely risk that information may be seized, limit yourself to oral exchanges and write the report later in a safe location. □ Write down only partial information and complete the full report as soon as possible in a safe location. □ Be sure to know what to say and how to conduct yourself in a situation in which sensitive information may be seized (raid, arrest, roadblock, checkpoint).
It may become known that the source provided information to your organization, which exposes him/her to harassment, retaliation or stigmatization		□ Choose an appropriate location if you are conducting interviews and confirm if the source feels safe there. □ Ensure that the victim or parent/guardian gives informed consent prior to an interview and knows how the information will be handled. □ Maintain a low profile when conducting interviews □ Coordinate closely with the UN to ensure that verification missions do not attract undue attention to the source. □ Identify partner organizations or entities able to provide physical protection to a victim/ witness at risk (e.g., relocation) and discuss this option with the victim/witness.
Other:		

Security and confidentiality when storing information

Assess your vulnerabilities - how high are the following risks for your office/organization and select relevant mitigating steps according to the level of risk:

Risk	Level (high/ medium/low)	Suggestions
Damage to premises (and documents) due to natural event/disaster		□ Keep copies of electronic and paper files in a different location. □ Reduce the amount of information you store in that location, for instance by archiving old files elsewhere (other office or overseas) every couple of years. □ Consider storing all information elsewhere. □ Make sure you list relevant steps in a contingency plan.
Searches/raids		□ Reduce the amount of information you store in one location, for instance by archiving old files elsewhere (other office or overseas) every couple of years. □ Keep copies of electronic and paper files in a different location. □ Consider storing all information elsewhere. □ Store hard copies in a discreet but safe place if you feel a locked cabinet would attract too much attention during a search/raid. □ Make sure you list relevant steps in a contingency plan.
Robbery		□ Store hard copies in a locked cabinet or in a discreet place if a locked cabinet would attract too much attention in a robbery. □ Do not store files in valuable items (laptops) or make sure you remove the items from the premises at closing time. □ Store electronic files in a mobile device that you can remove from the premises. □ Destroy all files as last resort (deletion, shredding, incineration). □ Assess office security and strengthen it if necessary. □ Keep copies of electronic and paper files in a different location.
Sudden closure of premises due to impending attack		□ Consider storing all information elsewhere. □ Store electronic files in a mobile device that you can easily remove from the premises. □ Remove files from the premises before closing the premises. □ Destroy all files as last resort before closing the premises (deletion, shredding, incineration). □ Keep copies of electronic and paper files in a different location. □ Make sure you list relevant steps in a contingency plan.
Electronic surveillance		□ Password-protect or encrypt electronic files. □ Change the passwords at irregular intervals. □ Restrict the number of people allowed to access the information directly. □ Make sure your computer has a functioning firewall.
Other:		

Security and confidentiality when sharing information with MRM focal points

□ Clarify the format and mode of communication: avoid sending sensitive information electronically or use caution if you must do so (firewalls do not protect documents sent out electronically): password-protect all documents and/or use a secure file-sharing platform.

□ Clarify what information you can share with the MRM focal point and whether codes or code words will be used.

□ Clarify who from your organization is authorized to provide information to the MRM focal point.

□ Clarify who at the UN is the MRM focal point who will receive your information.

□ Establish a confidence-based relationship with your MRM focal point.

□ Clarify how the UN will manage information provided by your organization (where will it be stored, how will it be communicated within the MRM).

□ Consider having a formal information sharing protocol with the UN detailing all the points above.

Institutional documents and policies you may need to develop or adapt depending on how you participate in the MRM

Documents	Key points
Staff Code of Conduct (and implementation policy/protocol)	• Behavior when collecting sensitive information. • Behavior when discussing sensitive information. • Abidance by internal protocols and plans.
Internal data protection protocol [See useful resources from the Child Protection Information Management System below]	• Who collects information? • How is information transferred from the field to the main office? • Who else can have access to information within the organization? • Who analyzes information? • Who communicates information to external actors? • What codes and code words are used? • Where is information saved and stored (paper, electronic)? • Who has access to passwords and keys? • Contingency plan for emergencies: what steps should be taken, who is responsible?
Include information management in the organization's safety and security plan	• Include preventative steps to store sensitive information safely. • Include a contingency plan to remove or dispose of sensitive information in the event of an emergency.
Client information / consent form	• Give options for consent on how the information can be used and who can access it.

related tools

- tool 44 – Annotated sample case database
- tool 43 – Q&A 'Using a case database'
- tool 29 – Checklist 'Confidentiality'
- tool 30 – Checklist 'Informed consent'
- tool 46 – Group exercise 'Confidentiality and information management'

other resources

- *Child Protection Information Management System, Training Manual* (Template data protection protocol and data protection checklist) available at **www.childprotectionims.org**.
- *Minimum Standards for Child Protection in Humanitarian Action*, Global Child Protection Working Group, 2012 – Standard 5 'Information Management'.
- *Security in a Box: Tools and Tactics for Your Digital Security*, Tactical Technology Collective and Front Line Defenders.
- *Workbook on Security: Practical Steps for Human Rights. Defenders at Risk*, Front Line Defenders, 2011.