9. ORGANISATIONAL SECURITY

> CHAPTER 1.8 OF THE NEW PROTECTION MANUAL
  IMPROVING SECURITY AT WORK AND AT HOME

> CHAPTER 2.1 OF THE NEW PROTECTION MANUAL
  ASSESSING ORGANISATIONAL SECURITY PERFORMANCE: THE SECURITY WHEEL

> CHAPTER 2.2 OF THE NEW PROTECTION MANUAL
  MAKING SURE SECURITY RULES AND PROCEDURES ARE FOLLOWED

> CHAPTER 3.1 OF THE NEW PROTECTION MANUAL
  REDUCING THE RISKS ASSOCIATED WITH OFFICE SEARCHES AND/OR A BREAK-INS

LEARNING OBJECTIVES

> Assess the overall security management of an organisation (or community).
> Improve compliance with security rules within the organisation.

KEY MESSAGES

> To assess your security, you need a two-fold approach: self-assessment and assessment of how others perceive you.
> Security is everybody’s business.
> Developing an organisational security culture is fundamental for the respect of security rules and protocols.
> Rules are observed only if they are understood and if everyone feels ownership of them.
> Successful security management requires time and resources.

THE SESSION

⚠️ CHALLENGES THAT MAY ARISE DURING THE SESSION:

→ The emergence of complexities and sensitivities associated with the dynamics of organisations.
→ Complex information and concepts.
→ Taking into account the specific protection needs that women HRDs and any other relevant social category of HRDs (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.) may have in terms of strategies, security norms, etc., both for routine protocols and emergency procedures.
→ This session only applies to urban organisations. If you are working with grassroots or community-based organisations in rural areas, we recommend you focus exclusively on the Observation of rules and security protocols section below while ignoring the case analysis. The discussion of the statement works well for such a session, but you should take into account the characteristics and needs of these organisations (See Chapter 5.8 of this guide and Guía Cuidándonos).
**THE SESSION STEP BY STEP:**

<table>
<thead>
<tr>
<th>Time</th>
<th>Acc. time</th>
<th>Activity</th>
<th>Tool / method / materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>15’</td>
<td></td>
<td>Introduction:</td>
<td>Have the points ready on a flipchart (or PowerPoint slide)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The learning journey</td>
<td>Enlarged print-out of the capacity-building journey on protection (Chapter 3)</td>
</tr>
<tr>
<td>65’</td>
<td>80’</td>
<td>Security wheel</td>
<td>Enlarged drawing of Security Wheel (or slide)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Explanation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Activity 1: Filling in the Security Wheel</td>
<td></td>
</tr>
<tr>
<td>60’</td>
<td>140’</td>
<td>Observation of rules and security protocols</td>
<td>Flipouts of cases (below). Flipcharts Markers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Discussion of the statement</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Explanation of security rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Activity 2: Case analysis</td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>215’</td>
<td>Improve security at home and at the office</td>
<td>Table “Checklist: Office Security Review” (NPM, Chapter 3.1). Example of a search warrant (can be fictional but should be realistic) Locally applicable laws governing legal searches (if possible) Flipchart Markers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Explanation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Activity 3: Analyse the security of participants’ offices or homes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Activity 4: Role play</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>230’</td>
<td>Conclusion</td>
<td></td>
</tr>
</tbody>
</table>

**TIME KEEPING: CALCULATE 270’ (4 HOURS AND 30 MINUTES), INCLUDING TWO 20’ BREAKS**

---

**LEARNING ACTIVITIES**

**INTRODUCTION: THE LEARNING JOURNEY**

Show participants a map of the journey they have been on so far. For this you should bring a print-out of the illustration of the capacity-building journey on protection (*Chapter 3 of this Guide*) and put it up on a wall, or project it. The tools covered in the training sessions are represented by symbols that appear along the path of the journey. Make sure that everyone feels confident in using the tools, and allow some time for clarifications if required.

Next, shift the discussion onto the organisational aspects of security management, i.e. how organisations work, how decisions are taken and how change occurs. Remind participants that successful security management is about changing attitudes and behaviour. While the training may have already achieved a certain degree of attitudinal change, it is their behaviour as individuals and how the organisation operates on a daily basis, that need to be consciously worked on.

Remind participants that the existence of a security plan does not automatically ensure security or protection. Invite participants to express their views on this, as it will help you steer the discussion in the right direction. Facilitators should point out that security requires ownership of the whole process, starting with an assessment of the current levels of organisational security, identifying where improvements could be made, implementing security plans, and eventually conducting a regular monitoring and evaluation process.
Introduce the Security Wheel by putting it up on a flipchart or projecting it. Explain the eight components, or dimensions, of the wheel (NPM 2.1, pp. 132-133). Once participants are familiar with the tool, explain the “step by step analysis of the Security Wheel”, i.e. the questions that need to be asked in order to determine the degree to which security components are currently met and any improvements that might be required or advisable (NPM 2.1, pp. 134-138). The logic behind the Security Wheel is that it should be as round as possible so that, if an actual wheel, it could roll easily. Translated into terms of security management, this means that it is not helpful to score well in one area but badly in others. All areas should be even.

**ACTIVITY 1: FILLING IN THE SECURITY WHEEL**

Ask participants to apply the analysis to their own organisations. Divide participants into groups if necessary (in this case, several security wheels will be produced for the same organisation). After all groups are finished, they should compare the different security wheels. Conclude the activity by engaging participants in a plenary discussion on the results of the exercise.

→ When working with a homogenous group (assuming you have not divided the participants into smaller groups for this exercise), discuss the meaning of each dimension (spoke) of the wheel (NPM 2.1) in plenary; otherwise provide instructions before group work begins. The area of each spoke should be shaded, successively, according to the current status of organisational practice. There is likely to be some disagreement and discussion around what percentage of each section should be shaded. Help the group to achieve consensus by emphasizing that the wheel is a tool designed to illustrate the current state of the organisation, as a starting point for organisational change. Finally, recommend that participants review the wheel in six-months’ time in order to assess their progress.

→ If participants have been divided into groups, ask those who work at the same organisation to work together. Then put all the results on the wall and discuss the following general points: the group(s) is (are) likely to obtain a wheel whose spokes have different areas shaded. This helps to identify the types of action that need prioritising to improve the organisation’s protection and security.
DISCUSS THE FOLLOWING STATEMENT

“The security of our organisation is only as strong as our weakest link.”

Read this statement to participants and present it on a flipchart too and encourage a discussion in plenary. The statement is based on the logic that if potential aggressors want to obtain more information on, or even harm, HRDs, they will probably try to find the weakest link that they will then act upon, for example, getting close to someone who likes to get drunk on Saturday nights. Similarly, if someone is interested in scaring the staff of an organisation, they will probably target someone who is generally careless about her/his security. Similarly, a careful person might be attacked because a careless person has left the door open. The point is that one careless person can put the whole organisation at risk.

EXPLANATION OF SECURITY RULES

Prepare and deliver a brief presentation on how security rules should be defined and supervised (NPM 2.2). This will provide the basis for the case analysis.

ACTIVITY 2: CASE ANALYSIS: HOW GOOD ARE THE RULES?

You can carry out this activity, which asks to participants to analyse three security rules of a fictional organisation, either in plenary or by dividing participants into three groups. Distribute one security rule (see below) to each participant or the group and ask them to analyse them according to the following criteria: practicality, sustainability, inclusivity and effectiveness. Note that the phrasing of the rules is intentionally convoluted, as the aim is to provoke discussion among participants about whether they are adequate and to identify improvements.

Allow participants to work for 10 minutes and then ask the plenary – or the groups if participants have been divided up – to report their analysis of the rules and then encourage a discussion in plenary (see Tips for Facilitators). If you wish, you may use examples taken from the organisation’s own security rules (but be careful, as this may create tensions).

→ RULE 1:

Before initiating verification of a presumed human rights violation, you should check the relevant parts of the security manual to make sure everything is being done according to the rules. If you are not familiar with the security manual because you are new to the job you should ask for help from your workmates or your direct supervisor.

→ Positive aspects:

• The rule refers to a security manual, which means, at least, that the organisation has one. As a rule, everybody should be aware of its existence.
• It implies that someone is responsible for security issues, i.e. the direct supervisor, to whom new staff can ask security-related questions. However, having to ask could be a barrier. If the organisation has an open consultative culture (meaning that people - and above all management - show a certain willingness to help), this should not be a problem.

→ Negative aspects:

• New staff should not have to take on such tasks. If they are required to, they should be properly trained and supervised.
• The security manual should be easily accessible, which does not seem to be the case here.
• Staff should know which parts of the security manual to consult. If it takes time to find the right
sections, people are likely to become discouraged and fail to follow the rule.

• The rule implies additional work, and this might lead people to ignore it.

• Two more general questions can be asked: does the rule make sense within the working context of the organisation? Have all staff members participated in drawing it up (thus encouraging ownership)?

• Finally, the human aspect of the work should not be forgotten. The rule could lead to a bureaucratised approach to people who come to the organisation asking for help.

→ RULE 2:

The country field office is responsible to the international headquarters in Geneva for the security of its local staff. Given the situation in the country, field trips to remote and high-risk areas represent one of the most vulnerable moments in terms of security. Therefore, the organisation’s international security standards, which must be applied in every country, require local staff to:

• Prepare each field trip to high-risk areas properly, at least seven days in advance. Before travelling to the field staff should meet in order to review the relevant protocols covering the preparation of field trips (check the security manual). The field trip will not be carried out, under any circumstances, if all requirements are not met.

→ Positive aspects:

• The reference to international standards clearly implies the importance of the rule.

→ Negative aspects:

• The seven-day rule might be an obstacle. Also, in regions were the security situation is unstable and fragile, the rule might be insufficient, as the security analysis carried out on one day might not be valid the next.

• It might not be realistic to think that all team members will always be able to meet before trips. This might have an impact either on the enforcement of the rule (members circumventing it on occasions) or on the work of the organisation itself (meaning there is a risk that trips will be cancelled because of the rule).

• The way to involve new staff in the design of security rules and to encourage ownership is to include them in analysing and periodically assessing the rules. In organisations with a top-down decision-making process, staff should at least be able to give feedback on the real viability, efficiency and adequacy of the rules. In more inclusive organisations, staff will be able to participate in assessing and deciding on security rules. It might not be easy to strike a balance between participation and the efficient use of resources. The rules should be reviewed periodically, but care should be taken to avoid making changes too frequently, as this can lead to staff ignoring the rules. Notwithstanding these aspects, emergency situations can sometimes oblige organisations to redesign a rule quickly.

→ RULE 3

During field missions away from the city, security considerations should cover free time, both in the evenings and at weekends. All the organisation’s staff must follow the following rules during their free time:

• You must not be on the street after 9 p.m., by which time you should be at your usual home or, if you are staying at a different house or a hotel, report to the person in charge. If you have a mobile phone, it must be operational at all times.

• Regional staff will define which places must not be visited after 9 p.m. for security reasons.

• Alcohol and other drugs must not be consumed.
Personal actions that might compromise other people’s security or the image of the organisation are not allowed.

Positive aspects:
- Overall, it is good that the rule deals with issues related to free time and security and takes into account times when staff are not officially working.
- Dangerous zones are defined, which makes it easier to avoid them.
- The rule also deals with issues related to alcohol and drugs, which may not be easy to address in some cultural contexts.

Negative aspects:
- Security issues related to drugs and alcohol should be better explained. Organisations should avoid referring to moral standards, but instead address the issue in a security-oriented way. Emphasis should be put on vulnerability and responsibility. It should be clear that if something happens, staff members need to be prepared to react. In some cases it might be easier to ensure compliance by setting a low level of alcohol consumption, while prohibiting the use of any illegal substances.
- In general, the rule does not explain the reasoning behind it. Such a rule-bound focus might make it harder to enforce. It could be good to provide a fuller explanation of why it should be respected. The principal problem is that the surest way to get someone to do something is to ban it.
- The criteria and requirements that have to be met before authorisation to travel is given are not clear, and the member of staff responsible for authorisation is not specified. The rule should also refer clearly to the relevant section(s) of the manual.
- Finally, it could be argued that the last point, on personal actions that might compromise the security of others or the organisation’s image is rather vague. The type of actions – or the situations in which they might take place - are far from obvious and could require further clarification.

IMPROVE SECURITY AT HOME AND AT THE OFFICE

Explanation
Base your explanation on the NPM (Chapter 1.8). The main security objective should be to prevent unauthorised access to the workplaces or homes of HRDs. Assessing office security is similar to conducting a risk analysis. The process uses the same concepts of threat, vulnerability and capacity. Highlight the fact that the vulnerabilities of an office must be assessed in the light of the threats faced and that, echoing the discussion about the observation of security rules, the security of an office is only as great as its weakest link.

Activity 3: Analyse the Security of Participants’ Office or Home
Ask participants to analyse the security of their offices using the table provided in the NPM (Checklist: Office Security Review, p. 94). Divide participants into groups if necessary. Encourage participants to discuss their analyses to close the exercise. If you are working with mixed groups, ask participants from the same organisation to work together.
**ACTIVITY 4: ROLE-PLAY: LEGAL SEARCH**

Four people are assigned the following roles (these roles must be adapted to each context and to the current laws of each country):

→ Judge, with a search warrant (adapted to the context).
→ 2 policemen searching the place.
→ 1 individual, with no identification papers, who hides a plastic bag full of cocaine and “finds it”.

Other participants are members of the organisation; their role is to decide on the reaction to the search.

When the role-play is over it should be evaluated. Base your feedback to participants on the concepts and elements found in **NPM Chapter 3.1**.

→ Inquire about the framework covering legal searches in the country you are working in. Print them out and hand them out to participants at the end of the role-play.

→ During the analysis of the role-play, ask participants how they felt during it. Insist on the fact that they will feel safer if they are familiar with the legal framework and are aware of their legal rights.

→ Divide the evaluation process into three phases (this needs to be adapted depending on the exact terms of the law):
  - Actions to be taken before the search: inquire about your legal rights; review security protocols - especially concerning the secure management of information (**NPM 3.1**); train members how to react when faced with a search warrant;
  - Actions to be taken during the search: call a lawyer (or someone you are sure will answer and who will be able to call a lawyer and other useful people); review the search warrant to make sure that it is legal; do not let the police officers enter the building unaccompanied (this will depend on your legal rights to refuse to leave the premises when ordered to do so by the police); be aware of anything illegal that the law enforcement officers may do;
  - Actions to be taken after the search: Make sure that everybody is fine; assess the search; design a plan to react to it and to limit its negative impact.

**CONCLUSION**

→ Ask participants to recall the key learning points of the session. Insist on the key messages by referring to issues or examples that have been mentioned during the day.

**ADDITIONAL RESOURCES**
