

Making sure security rules and procedures are followed

Purpose:

To think about what makes members and organisations unable or unwilling to follow security plans and procedures, and find appropriate solutions.

Security is everybody's business

Whether people and organisations actually follow security procedures and rules is a complex issue. It is quite possible to have a good security plan, complete with preventive rules and emergency procedures, and have security placed high on agenda at all major meetings, etc, and yet have people still not complying with the organisation's security rules.

This may sound incredible, given that human rights defenders are constantly under pressure and threats, but it does happen.

If someone wants to know something about your work, they will not try to find out from the most careful person in the organisation. Rather, they will try to get close to someone who often gets drunk on Saturday nights. Similarly, if someone wants to give your organisation a fright, they probably will not assault a person who has taken all the necessary precautions. Rather, they will probably target someone who is usually quite careless about their own security. Similarly, it could be that a careful person is attacked because the careless person left the door open... The point is that one person's carelessness can place everyone at greater risk. Security is only as good as the weakest of its underlying elements -in this case to the negligence of one individual.

This is why security should be defined as an issue for the whole organisation, as well as for the individuals it involves. If only three out of 12 people follow the security rules, the whole organisation, including those who observe the rules, is put at risk. If the situation improves and nine people start following security procedures, the risk is reduced. But the risk would be smaller still if all 12 people followed the rules.

**Security is an issue for
the whole organisation,
as well as for
the individuals it involves.**

Having a good security plan is meaningless unless it is being followed. Let's be realistic: many people do not follow rules or procedures. The lack of compliance amounts to the difference between good intentions and actual practice. It is nevertheless easier to confront this problem than its possible consequences.

Why do people fail to follow security rules, and how can we avoid this from the outset?

First of all, the word "compliance" carries connotations of submissiveness and docility and should therefore be avoided. People only follow rules that they understand and accept, because they can then make them their own. Therefore, the key word here is "ownership".

In order for a security procedure to be followed, everyone in the organisation has to embrace it. This doesn't happen instantly. In order for group members to embrace a security procedure they must be allowed to participate in drawing it up and implementing it. Training, understanding and acceptance of the procedure are also crucial.

Table 1: The relationship between individuals and organisations in security terms

CONCEPT	APPROACH: "EVERYONE MUST FOLLOW THE RULES!"	APPROACH: "THE INDIVIDUAL AND THE ORGANISATION HAVE AGREED ON THE RULES!"
APPROACH	Rule-focused	Based on organisational and personal security needs
TYPE OF RELATIONSHIP BETWEEN THE INDIVIDUAL AND THE ORGANISATION	Normative or "paternalistic"	Based on dialogue
WHY DO WE FOLLOW THE RULES?	By obligation, to avoid sanction or expulsion	To observe an agreement, with room for criticism and improvement (ownership and persuasion is achieved when we are convinced that it fits our needs and it will decrease the feasibility and consequences of a risk and it will contribute to protect our colleagues and the people we work with/for)
RESPONSIBILITY FOR SECURITY	Not shared	Shared

Ownership is not just about "following rules", but about establishing an agreement about the rules that will make individuals follow them because they understand them, see them as appropriate and effective, and feel they have a person-

al stake in them. For this reason, the rules should also conform to individuals' moral and ethical criteria and basic needs.

**Ownership is not about simply “following rules”,
but about respecting an agreement between the organisation and
group members regarding security.**

In order to maintain the agreement between group members and the organisation it is important that **the individual(s) responsible for security** should **keep others constantly involved** through briefings, reminders about aspects of the agreement, and by asking people's opinions on how appropriate and effective the rules are in practice.

Such involvement will however be of little value without an **organisational culture of security** which underpins formal and informal work procedures or programmes.

In summary, the necessary basis for people to observe security rules and procedures can be achieved through the following steps:

- ♦ Developing an understanding that security is important for the protection of victims, witnesses, family members and colleagues, to enable the core work of the organisation to continue;
- ♦ Developing and valuing an organisational security culture
- ♦ Creating ownership of security rules and procedures;
- ♦ Making sure all group members participate in designing and improving security rules and procedures;
- ♦ Training people in security issues;
- ♦ Making sure all group members are convinced of the appropriateness and effectiveness of security rules and procedures;
- ♦ Drawing up and concluding an agreement between the organisation and individuals about respecting security rules and procedures;
- ♦ Involving those responsible for security in briefing and training people, in reminding group members of the terms of the agreement and in asking their opinions on how appropriate and effective the rules are in practice.

Why security rules and procedures are not followed

There is no prototype of a human rights defender who doesn't follow security rules. Many people within an organisation often follow some rules but not others, or observe the rules sporadically.

There are many possible reasons why people don't observe the rules and procedures. To change this and ensure ownership, it is important to establish the causes and find solutions alongside the other people concerned. It will also be useful to distinguish between the different reasons people may have to not follow the rules, because they will vary.

Some possible reasons for not observing security rules and procedures:

Unintentional:

- ◆ The defender is unaware of the rules;
- ◆ S/he doesn't apply the rules properly.

Intentional:

General problems:

- ◆ The rules are too complicated and difficult to follow;
- ◆ The procedures aren't within easy reach in the office or are presented in a way that makes them difficult to use day-to-day.

Individual problems:

- ◆ The rules are at odds with the individual's needs or interests and this conflict hasn't been resolved;
- ◆ The individual does not agree with some or all of the rules and considers them unnecessary, inappropriate or ineffective based on personal experience, previous information or training or because of personal beliefs.

Group problems:

- ◆ Most group members don't follow the rules, or group 'leaders' either don't follow them or don't do so enough, because there is no organisational security culture;
- ◆ A general lack of motivation at work can lead people to ignore security rules.

Organisational problems:

- ◆ There aren't sufficient financial or technical resources to make it easy for group members to follow the rules;
- ◆ There's a contradiction between the rules and particular areas of work. For example, rules have been established by those in charge of security but ignored or not properly implemented by people working in programmes or accounts. Some rules might suit one work area and contradict another;
- ◆ Group members and staff have a heavy workload and limited time, and don't prioritise some or all of the rules;
- ◆ A general lack of motivation, arising as a result of stress, workplace disputes, etc.

Organisational culture is both formal and informal, and must be developed not just in the organisation as a whole, but also in teams. A good organisational culture will be revealed in signs such as informal chatting, joking, parties, etc.

Monitoring the observance of security rules and procedures

Direct monitoring:

Security rules and procedures can be incorporated in general work appraisals and “check-lists”; as well as in meetings before and after field missions, in work reports, on meeting agendas, etc.

Periodical reviews can also be carried out together with the teams in question, of issues such as the safe-keeping of sensitive information, copies and security manuals; of security protocols for visits to the organisation’s headquarters; preparing to go on field missions, and so on.

Indirect monitoring:

Asking people for their views about rules and procedures, whether they are appropriate and easy to follow, etc, can establish whether the group members actually knows the rules, whether they have been fully accepted or if there is some disagreement which should be dealt with.

Group members usage of the security manual and any existing protocols and rules can also be reviewed.

It is worthwhile to compile and analyse, along with the people or teams in question, people’s opinions and evaluations of security rules and procedures. This can also be done off the record/anonymously or via a third party.

Retrospective monitoring:

Security can be reviewed by analysing security incidents as they arise. This must be handled especially carefully. Someone who has experienced a security incident might worry that it was their fault and/or that analysis will lead to sanctions against them. S/he might therefore be tempted to conceal it, leaving the incident, or aspects of it, unreported.

Who does the monitoring?

Depending on the way the organisation operates, whoever is responsible for organising security, specific areas of work within security and managing any security group members, will also be in charge of monitoring security.

What can we do if security rules and procedures aren’t being followed?

- 1 ♦ Establish the causes, find solutions and put them into practice. The list of options in Table 1 above can be used as a guide.
- 2 ♦ If the problem is intentional and only involves one individual, try to
 - a • engage in a dialogue with the person to establish the cause(s) or motive;
 - b • work with the individual’s whole team (this can sometimes be inappropriate, depending on the case);

- c • apply a notice or warning system, so that the person is fully aware of the problem;
- d • use a system of gradual sanctions which could culminate in the person being sacked.

3 ♦ Include a clause about observing security rules and procedures in all work contracts, in order for all staff to be fully aware of how important this is to the organisation.

In conclusion...

Some may argue that a discussion of the reasons why people don't follow security rules is a waste of time, as there are more urgent or important things to be done. Those of that opinion usually believe that rules are simply there to be followed, full stop. Others are aware that the world doesn't always work that way.

Whatever your opinion, we now invite you to step back and analyse the degree to which security rules and procedures are being followed in the organisation(s) where you work. The results could be surprising and worth spending time on, in order to avoid problems further down the line...

Summary

Security is everybody's business

Security is an issue for the whole organisation, as well as for the individuals it involves.

The reasons why people do not follow security rules need to be established; they may be:

- unintentional (individual problem)
- intentional (general, individual, group, organisational problems)

Knowing them will contribute to finding appropriate ways to handle them. However, monitoring through an appointed body is recommended (direct, indirect and retrospective monitoring).

Developing an organisational culture of security is fundamental