

Secure management of information

Human Rights defence organisations manage information that in an environment hostile towards defenders could be used to affect the safety of the organisation, other people and institutions. It is therefore crucial to set up a secure information management procedure and a reaction plan to any incident affecting the security of information managed by the organisation.

Secure management of information: prevention procedure

Data held by HR organisations may in general terms be grouped into two categories according to its level of sensitivity: high confidentiality, and low confidentiality.

Any piece of information managed by us undergoes four separate steps before reaching us and before leaving is (where relevant). We will outline the security needed at every step along its way.

- 1 • Source- information collection, at meeting point.
- 2 • Transfer of the information,
- 3 • Processing and storage.
- 4 • Distribution.

1 • Source- information collection at meeting point.

The main problem here is protection of the information and the people affected by it.

The person living the information requires a route between their home / office and the meeting point; a meeting point (the place where the person giving the information meets up with a member of the organisation); this meeting point may be that person's home or place of work, the organisa-

tion's offices or any other place; and a route to leave the organisation's headquarters (trips to and from the meeting points).

A secure place and conditions for meeting are required, as well as a route for the information to arrive and leave the source, and a route for the arrival and exit of members of the organisation who will in turn transfer the information.

Information management security begins even *before* receiving it.

- Does the organisation even need to obtain this information?

Will the organisation be able to use the data to improve its work or better meet its aims and objectives? If not, it is better that the organisation **does not receive** the information; if it falls outside its sphere of competence, our organisation may refer the person to another organisation, without taking on either the information or the case.

- Communicate to the person giving the information who we are, what our objectives and work are, how the information will be managed by the organisation; the sort of information we require, how we will look after it and use it- and what they can expect from us. It is fundamental and ethical that the person giving the information should know in advance (either directly or via third parties) the risks of passing on the information, and the uses to which the organisation might put it.

It is not enough to suppose that the person concerned is aware of all this. It is important for us to explain it to them so that we are sure that he/she knows it. It is also important to define with them possible security measures.

The meeting place must be as secure and anonymous as possible. In all likelihood the person's home will not be a secure place, as the arrival of an organisation staff member would be easily noticed. The organisation offices may offer more security (as long as confidentiality is respected), or another fairly public place in which people are coming and going routinely (e.g. parish building, community centre) as long as confidentiality is once again respected. If the meeting is arranged in inappropriate place, it may be adjourned to a more secure location according to the sensitivity of the information being transmitted.

One might also consider resorting to an official cover story: the person leaves home with an official pretext. They will need to build the pretext: dentist visit (show tooth ache), medical visit (any illness), market, etc the person will need to come back home with real proof (medical prescription and drugs, shopping that they would not have found in their home place)

Do not forget that security problems may arise for the person giving the information after the meeting at the agreed meeting place.

2 ● Transmission of information

Information may be gathered in various mediums: memory, printer, notes written by hand or on the computer, photos, etc...

The most secure routine method of transferring information is by laptop computer, memory stick or CD Rom equipped with security encryption. The meeting can be recorded, photos can be stored and notes can be taken. All other mediums are deemed to be less secure, which increases the risk of the transmission process.

Confidential information should be carried only by organisation members who are aware of what they are carrying.

Too often human rights defenders travel with their whole note books containing important information not necessarily related to the specific mission. They keep the notebook until it is full instead of travelling with only the amount of paper or material they need. The same goes for the content of USB flash disks, computers and other information support.

3 ● Storage and processing of the information

Once the information has reached the offices of the organisation it is usually more secure (according to the weaknesses of the office- see chapter on security of houses and offices).

Standards of particular relevance to information are:

Paper archiving of printed documents: this should be used only where necessary; necessary documentation on particular cases should be handed over in person. Paper information should be stored in lockable metal boxes; the use of a strong room should be considered for storing these.

One may also consider the possibility of distributing the papers between several safe places or send them to other places with the same care as illustrated in "transmission of information". Information can also be scanned, encrypted and sent to a trusted body (for example, to an international counterpart).

Encryption systems and codes should be used appropriately.

Make weekly back-up copies, and store these copies, also encrypted, securely, in a safe or other place.

4 ● Distribution of the information

General criteria regarding the distribution of information include the following points:

- Cross check the information

- Where the organisation is the only source of information on certain facts, there will be increased risk and contingency plans will be needed.
- Informed consent should be obtained from the persons giving the information, particularly where these persons are identifiable locally as the only source of the information.
- Any written information leaving the organisation or allied organisations should be considered “public” due to the risk of it falling into the wrong hands, or the day to day vagaries of means of communication.
- It is crucial for the organisation publishing the information to have a dedicated publication policy; this should include the main security standards applicable to the publishing of the information (among which rules to word the information itself).

Access to information by persons who are not members of the organisation (helpers, volunteers, etc...)

For the safety of the organisation, third parties, helpers and volunteers, access to these digital and physical archives must be restricted (decide according to the type of case) and must come under the particular responsibility of a staff member of the organisation.

It may be useful to incorporate into the contract or work agreement documents of helpers and volunteers a confidentiality clause that should be abided by at all times. This confidentiality clause should also be included in contracts of personnel subcontracted by the organisation.

Secure data management: reaction procedure in cases of theft or loss of the data.

Theft or loss (it may be hard to determine which it is) of data held by the organisation should cause us to react as though the information will necessarily fall into the wrong hands, and that malicious use will be made of it, that may affect third parties (whether those reporting the information or colleagues, etc...) or the organisation itself.

If, despite all the prevention procedures, a loss or theft of information occurs, it should be treated as a serious security breach, and the following steps should be taken:

- 1 ♦ Immediately inform people at the organisation.
- 2 ♦ Assess the quantity and sensitivity of the information lost or stolen, according to whether:

it puts at risk the people directly affected by the information, third parties or the organisation, and why (or the vectors for risk). This assessment should be carried out for every type of information stolen, where several types were stolen (e.g. lists of people, references and information collected on individual cases).

- 3 ♦ Assess the subsequent informing of people and institutions potentially affected so that they may take appropriate steps to protect themselves (should always be done discreetly).
- 4 ♦ Assess informing the authorities and reporting the events.
- 5 ♦ Where necessary, set in motion any other steps needed to avoid damage in case the lost or stolen information might be used. .

The organisation will also need to decide how far its members can expose themselves to risk in order to protect information: for example in case of a violent search, one ought to consider if it is “worth” resisting.

Summary

Secure information management requires prevention and reaction protocols.

Prevention ought to consider 4 moments:

- 1 • Source- information collection, at meeting point.
- 2 • Transfer of the information,
- 3 • Processing and storage.
- 4 • Distribution.

Reaction ought to at least include:

- 1 • Informing the responsible persons in the organisation
- 2 • Assessing the quantity and sensitivity of the information lost or stolen
- 3 • Assessing the subsequent informing of people and institutions potentially affected
- 4 • Assessing informing the authorities and reporting the events.
- 5 • Steps needed to avoid damage in case the lost or stolen information is being used.