2.4 Exercise

Information ecosystem

Purpose & Output

The purpose of this exercise is to take an inventory of the most important information assets you manage, in order to create policies for its safekeeping later on.

Input & Materials

It may be helpful to reproduce the example table below, either by printing it or drawing it on a flip-chart or other materials.

Format & Steps

Brainstorming and documentation

To begin the exercise – especially in a group – it may be useful to use a spreadsheet, or a large sheet and sticky notes, or some other means which allow you to brainstorm easily and group things together.

Brainstorm and make a list of all of the data you manage. If you're not sure where to begin, consider:

- data related to each of your human rights activities
- personal data and files, especially if stored on your work computer
- browsing activities online, especially of sensitive data
- emails, text messages and other communication related to your human rights activities.

Imagine a spreadsheet that has several columns enumerating categories as described below. Your task is to fill the rows with information.

Start with your information at rest, and for each type of information, elaborate on the following

- what information is it?
- where does it reside?
- who has access to it?

Format & Steps

- how sensitive is it?
  - secret
  - confidential
  - public
- how important is it to keep it?
- who has access to it?
- how should it be protected?
- how long should it be kept before destroyed?

Characterise and qualify the information you have mapped out. You can repeat the same process and expand the spreadsheet with additional entries for your information in motion; e.g. data being transferred (physically, electronically), communications over the internet or telecommunications networks.
The questions and example in Table 2 below may help you with this.

Remarks & Tips

This process is iterative. Once you have done the first round, you may detect patterns and groupings. For instance, you may decide that since all financial information (regardless of type) has similar sensitivities and longevity, you can group them and think of them as a financial information category.
Conversely, you might find yourself needing to expand a row into several rows. For instance, a row containing ‘email’ needs to be expanded to several rows to account for a subset of emails – and their safe-keeping – which is sensitive.
This should be a live document and will change according to shifts and developments in your situation. So you will benefit from regularly updating this document to account for any of these changes.

Table 1.

Information at rest				
What (examples)	**Attributes**			
	Where does it reside?	**Who can/does access it?**	**How sensitive is it?**	**How should it be protected?**
Financial documents in electronic form	Secure shared folder – file server	Executive team	Secret	Saved in hidden encrypted partition. Backed up daily to encrypted hard-drive
Program reports for the censorship campaign	Documents folder – file server	Team members, program director	Confidential	Saved in encrypted partition
Adobe InDesign for the web developer	Web content manager's laptop	Web content manager	Confidential	Licensed, password-protected

Table 2.

Information in motion					
What (examples)	**Attributes**				
	What method of transfer are you using?	Who has (or wants) access to it?	What physical or virtual routes does it take (origin, path, destination)?	How sensitive is it?	How should it be protected?
General emails among team members	Email (Gmail)	Team members, email provider	**Origin:** staff computers **Path:** internet (via Google servers **Destination:** staff computers	Confidential	GPG encryption
Check-ins during missions	Text messages (SMS)	Team members, telecom company	**Origin:** mobile phone **Path:** mobile network **Destination:** mobile phone	Secret	Code words