Annex 5 Confidential Procedures

Draft Hivos Confidentiallity Procedure – version 051212

In general information about partners and contracts is public. This means that:

1. Information about the organisation and contract can be shared freely.
2. Hivos gives details on the organisation and the project in publications to which third parties have access, such as IATI Open Data, Hivos Online or the Hivos Magazine.
3. Information in the project administration is available for all Hivos staff.

In some cases however confidentiality must be observed in the relationship between Hivos and the CP. This can be at the request of the CP or decided by Hivos.

On the other hand it should be very clear for everybody that the security of electronic data on servers or in the cloud is not related to individual projects: the chain is only as strong as its weakest link. This means that:

- all offices of Hivos all over the world need to have the same security level;
- all staff needs to follow the same rules regarding the use of Remote Access funcionalities and the cloud;
- all staff needs to follow a set of rules when travelling also to a country or region where confidentiallity is not a direct issue.

Overall responsibility lays with ....

Approval

The need for confidentiality and the level have to be approved by HoB/dRO and recorded in a memo including argumentation. It is possible to classify groups of partners in their entirety as confidential, e.g. human rights partners working under very repressive circumstances, or even all partners in a certain country. The memo is archived in the safe. DPP, hTEC, Finance and if necessary ODR are informed orally after approval. The related measures are applicable to all involved departments.

If confidentiality is not absolutely necessary, but a CP does ask not to publish details on the project or organisation in public communications, this is allowed. After approval of the HoB/dRO the partner gets the confidentiality status and the reason is recorded in the project administration under organisation details.

Information to protect

If confidentiallity is applicable, the following kind of information should be handled treated as confidential:

- Names, addresses and other personal information of partners
- Nature of the project and/or activities

- Agenda's and minutes from internal meetings about partners of meetings with partners
- Agenda's, plans and reports from duty trips
- Information relating to the funding and donors
- Donor reports
- General reports and data overviews in which confidential partners are mentioned

Classifications and measures

Hivos has three levels of confidentiality:

1. Confidential
2. Highly confidential
3. Fully confidential

The classifications mean the following. HoB/dRO can decide to take additional measures.

Confidential:

1. Although available for internal use, information must be used with caution.
2. Hivos will not use any details on this organisation in publications to which third parties have access, such as IATI Open Data, Hivos Online or the Hivos Magazine.
3. No information related to the project and the partner is shared by staff with third parties in social settings (meetings, conferences, parties, et cetera) or by means of social media (blogs, twitter, et cetera). If necessary information can be shared within Hivos and with reliable partners and allies outside Hivos, but with the explicit request to keep it internal or confidential.
4. In the project administration **PA** gives the business partner and/or contract the confidential status. When the contract has the confidential status, automatically no information related to this specific contract is used in publications as described under point 2. When the business partner has the confidential status, no information of any related contracts is used in publications as described under 2, even if the related contracts are public.

Highly confidential adds:

5. Partner and contract related information is shared with relevant colleagues at Hivos only, with the explicit request to keep it internal or confidential.
6. Files are not open for other colleagues. Contract information should be stored at a separate part of the electronic drive supported by ICT. Access to this electronic archive is restricted to the program staff responsible for that partner or project.
7. Don't use the archiving modality of the project administration. To administer the receipt of reports, attach only the first page of reports or a memo in the project administration when they contain sensitive information.
8. Hard copy files of confidential partners are stored in a locked cupboard. Keys are kept only by staff responsible for that partner or project. The HoB/dRO keeps a list of key owners.

9. The involved staff needs to have a print code, so that prints are not left unattended at the printer.
10. A shredder needs to be at reach for destroying hard copy documents.
11. Careful communication by regular e-mail, do not use names in the email headings.

Fully confidential adds:

12. Partner and contract related information is shared with a small selection of involved Hivos staff only.
13. Names of activists are coded.
14. Communication via via hushmail or via shared accounts on hushmail or any other provider which is deemed sufficiently safe (please follow the advices from the Hivos IT department on this). Shared accounts are e-mail accounts which both sides use and have access to, but no third parties.
15. If for safety reasons a partner cannot receive emails at all leave the Email Address of the contact person in the project administration blank.
16. It is not allowed to take information outside the building, whether it is digital (laptop, stick, etc) or on paper.
17. For duty trips, see the chapter on High Risk Traveling and on Training below.
18. Payments can be done to a bank account in another country than that of the business partner.

ICT can be asked to give additional advice on data security.