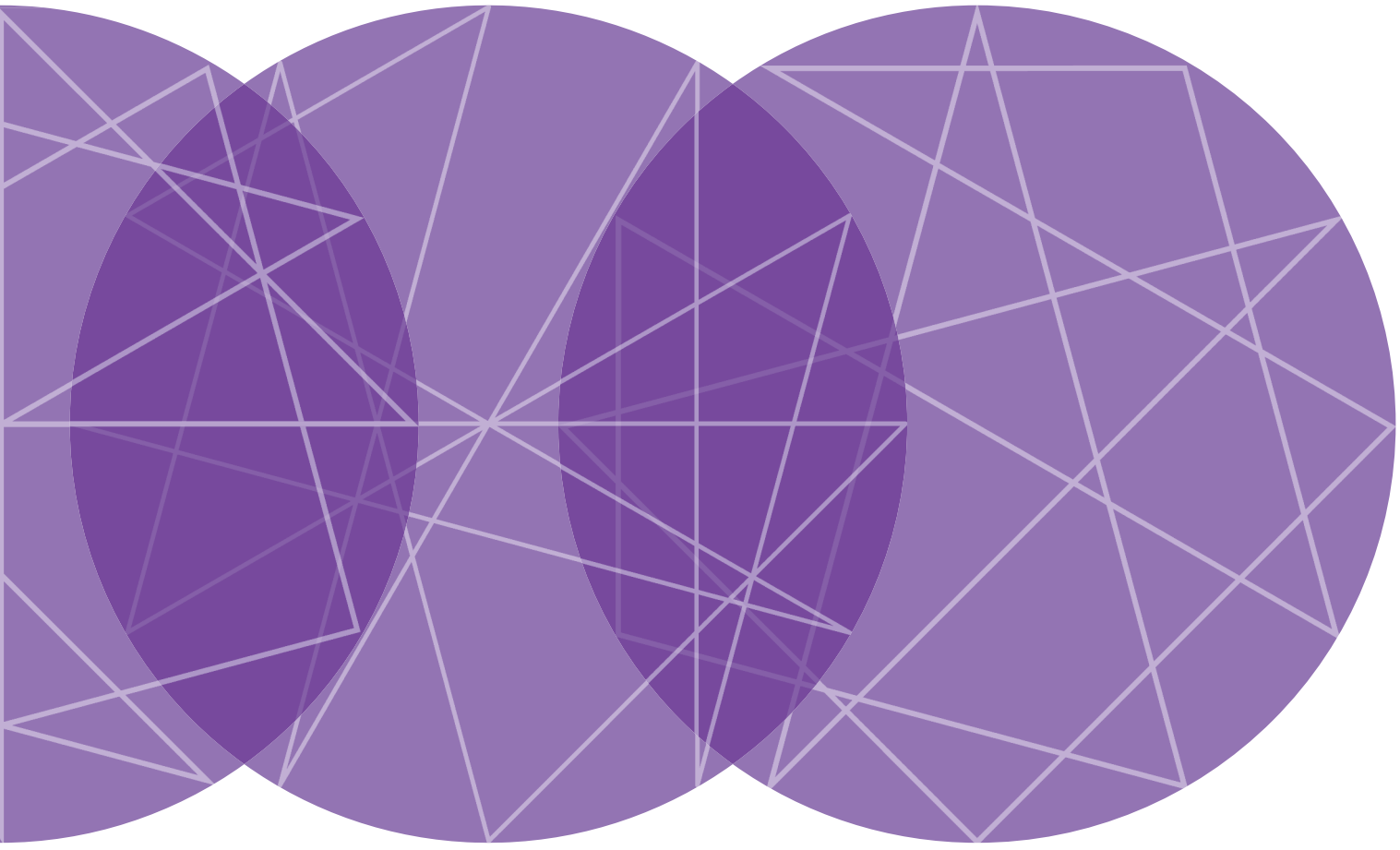
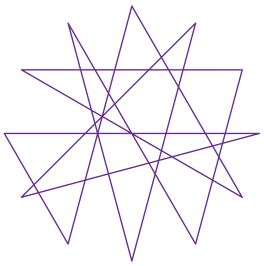
eisf

The Information Management Challenge: A Briefing on Information Security for Humanitarian Non-Governmental Organisations in the Field



European Interagency Security Forum (EISF)

eisf



European Interagency Security Forum

The European Interagency Security Forum is an independent platform for Security Focal Points from European humanitarian agencies operating overseas. EISF members are committed to improving the safety and security of relief operations and staff, in a way that allows greater access to and impact for crisis-affected populations.

The Forum was created to establish a more prominent role for security management in international humanitarian operations. It provides a space for NGOs to collectively improve security management practice, and facilitates exchange between members and other bodies such as the UN, institutional donors, research institutions, training providers and a broad range of international NGOs.

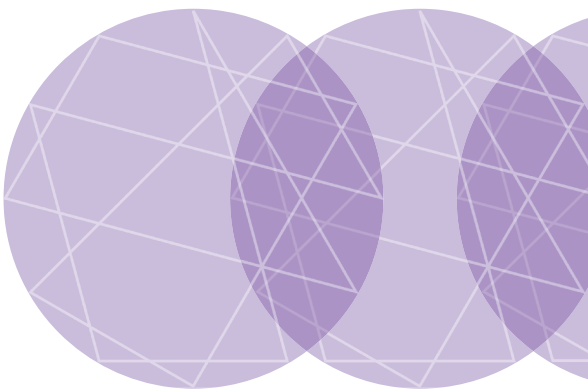
EISF fosters dialogue, coordination, and documentation of current security management practice. EISF is an independent entity currently funded by DFID and hosted by Save the Children UK.

Acknowledgements

This briefing paper was written by Robert Ayre, and edited by the EISF Secretariat.

EISF would like to thank the following, who contributed to this paper either through interviews or the peer review process: Andrew Anderson and Wojtek Bogusz of Front Line Defenders, Pete Buth of MSF-Holland, Heather Hughes and Jo Lyon of Oxfam GB, Trevor Hughes of International Medical Corps, Rafael Khusnutdinov of Save the Children US, Maarten Merkelbach of the Security Management Initiative and Richard Powell and Ian Trask of Save the Children UK.

While all provided important input and feedback, all errors that remain are EISF's alone.



Contents

1 Purpose

Information management in the field is a major challenge for NGOs delivering humanitarian assistance in emergency situations, highly-insecure environments or even in more stable, development contexts. NGOs will often collect, store and communicate sensitive information regarding their staff, partners, beneficiaries and programmes, and yet they may not have the systems, policies or procedures necessary to protect it to the standards adhered to at headquarters.

The objective of this briefing paper is to enable humanitarian NGOs to conduct an informed analysis of their information management practices in the field. It is based largely upon interviews with Security Focal Points and information managers in humanitarian NGOs.

2 Introduction

Delivering humanitarian assistance requires NGOs to collect, store, process and communicate reams of information, some of which is potentially sensitive. Sensitive information comes in myriad forms, from photographs to witness statements, financial reports to medical records. That it is collected, stored and communicated, however, raises the question of how its confidentiality is ensured.

"Information management" is the umbrella term used to describe policies and guidelines designed to: regulate the types of information organisations collect, store and communicate; reduce the risks to beneficiaries, staff and organisations inherent in these processes; and ensure that information can be accessed by the right people in a timely manner.[1] Information management is challenging in field conditions, but the legal and ethical duty of NGOs to ensure the confidentiality of sensitive information remains paramount. Fundamentally, failures in creating or implementing information management policies can have negative repercussions for staff, beneficiaries and organisations, and could result in legal redress.

That said, no humanitarian NGO is a "secret service". Much of the information collected is harmless in most circumstances. This paper is not designed to instil fear and overreaction. Too much security, restricting the effectiveness of programmes and leading potentially to self-incrimination, is feasibly as bad as too little. And if staff perceive security measures to be overly restrictive it is unlikely that they will be consistently observed. Good information management is in part about achieving the correct context-determined equilibrium between the benefits that collecting, recording and communicating certain sets of information brings or enables to beneficiaries, and the risks these actions entail.[2]

The ultimate objective for humanitarian NGOs should be the strengthening of an "information management culture", where information security is embedded in wider risk management policies and procedures, incorporated into organisational and programmatic thinking as a seamless process. Most risks can be mitigated through risk awareness, common sense and good discipline: what this paper terms good "housekeeping".[3] Information security is not a challenge to be addressed by IT departments alone. Strong "housekeeping" and good technical solutions are underpinned by effective staff training and sufficient resources, constituting a strong information management culture in which security policies are implemented almost subconsciously in the actions of staff.

Central to this organisation-wide culture is an effective set of information management guidelines. In general, such guidelines should:

- Aid the delineation of sensitive information from routine information in the particular context in question, using the programme's context analysis and risk assessment procedures.
- Suggest context-determined measures to protect against information loss, and to reduce the risks inherent in information collection, storage and communication, whilst ensuring that appropriate individuals have timely access.

1 Internal document provided by an NGO, 16 December 2009.
2 CIO Council 2009:6.
3 Interview, 29 October 2009.

- Measure risks against articulated risk thresholds to determine when information should **not** be stored.

This paper comprises a primer and four annexes. The primer seeks to outline the conceptual process an information management policy should inculcate in an organisation to ensure good information security practices. Annex 1 explains the information management process diagram in chapter 5 of the primer. Annex 2 shifts a degree toward the practical, providing an index for an information security policy. Annex 3 describes specific physical, digital and communication vulnerabilities, and corresponding mitigation measures. Finally, Annex 4 provides links to documents and websites that provide further detail.

Sensitive information defined

In general, sensitive information is: privileged information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organisation owning it, its staff, partners and/or beneficiaries.[4]

Most organisations, from pressure-groups to multi-national corporations, media outlets to government ministries, collect, record, process and communicate such sensitive information. All European countries regulate these actions through law.

The 1998 British Data Protection Act (DPA), concerned with the management of information on "data subjects" (individuals), is fairly typical. It stipulates that:

- The organisation collecting the information in question actually **requires** it for the purposes it has outlined to the Information Commissioner.
- The individuals about which data is collected **know** that the organisation in question is going to store personal information about them.
- Individuals are **aware** if the information is going to be passed onwards.
- The information is held **securely**.
- Access to the information is **limited** strictly to those who need to use it.
- The information is **deleted** as soon as it is no longer required.
- The organisation's staff are **trained** to understand their obligations under the DPA.[5]

That humanitarian agencies operate in challenging environments does not absolve them of responsibility for ensuring that, as best as is practicable, they live up to the obligations data protection legislation places upon them in the country of operation. Where host-country law is significantly less stringent than equivalent European law (for instance, in ensuring the confidentiality of medical records), NGOs may feel an ethical duty to adhere to the standards met in their headquarters.

Examples of the types of information that might be deemed sensitive include:

- Medical records
- Contextual information, such as situation and incident reports, that could be perceived as evidence of "spying" or be of use to belligerents or other local actors
- Advocacy investigation reports (including witness statements, photographs, emails or phone conversations discussing their content)
- Staff movements, especially where there is risk of kidnap or attack
- Minutes of meetings, whether internal or with beneficiaries
- Cash transfers
- Programme accounts and associated information
- Human Resources information (including CVs, salaries, next of kin, etc.)

What is "sensitive" is frequently context-dependent. Medical records are always sensitive, but they have the potential to be even more so in particular contexts. For instance, in a country whose culture prohibits pre-marital sex, unauthorised access to medical records identifying unmarried individuals as having sexually transmitted infections could lead to negative

4 Definition from Business Dictionary.com, available at: http://www.businessdictionary.com/definition/sensitive-information.html (accessed 20 November 2009).
5 Information Commissioner's Office, available at: http://www.ico.gov.uk/what_we_cover/data_protection/your_legal_obligations.aspx (accessed 20 November 2009).

repercussions for the named beneficiaries.[6] Minutes recording participants in and contents of discussions with community leaders regarding needs may be quite harmless in most contexts. Conversely, in a conflict situation where the community in question is accused of rebelling against the state, such minutes may be incredibly valuable to a government intent on silencing opposition.

Determining what is sensitive thus requires that information management is considered as a component of a programme's risk management procedures. Context-analysis, actor mapping and risk assessments can be used to identify sensitive information, as well as the degree of risk posed by each programme's associated files. Information security can thus become a key constituent of an organisation's risk register.[7]

Risk assessments should be performed whilst conscious of the fact that risks are frequently multi-faceted. In the example discussed above, in which minutes of a meeting with community leaders are accessed unauthorised by an armed group, a single Word document could: severely damage the reputation of the organisation in question locally; reduce staff security due to a backlash by the affected community; prevent a partner organisation operating in that vicinity again; and trigger negative repercussions for beneficiaries. Each risk, if it comes to pass, will have different impacts on different groups. Furthermore, if the information breach resulted from negligence or systemic failure, it could leave staff or the organisation open to legal challenge.

A note of caution is required, however. Quantifying risks flowing from the leakage or theft of information is often difficult. The degree to which surveillance or poor security practices were responsible for the expulsion of thirteen NGOs from Sudan in March 2009 is very challenging to accurately assess.[8] What is important is that the types of risks present (in this case prolonged government surveillance) are known and understood, and information security is as tight as is reasonable in the specific context. In this way risks – foreseeable or less so – will be reduced.

Aspects to the information management challenge

a. General

The challenges associated with information management are many and varied. As noted above, "information management" is a broad term, encompassing a wide range of issues. One, however, appears to underlie many of them: even as technology grows more powerful and complex, the source of the majority of vulnerabilities exposing sensitive information to unauthorised or malicious access seems to be basic failures in "housekeeping".[9]

Good housekeeping is where awareness, common sense and discipline combine with an effectively formulated and communicated policy to create a continuous, near-subconscious implementation of fundamental security procedures. Too often, it appears, good housekeeping is neglected. Sensitive documents are sent to print and subsequently left idle on printers for extended periods; staff fail to identify what is "sensitive" and take no extra precautions to protect it; anti-virus software is not installed; and no one is quite sure of the number and locations of office keys in circulation.[10] One interviewee estimated that basic failures in housekeeping were "eighty percent" of the information management issue.[11]

A factor underlying poor housekeeping can be lack of capacity: staff without a high level of IT skills may simply be unsure of available methods for protecting the information they record and communicate. Hence, agencies should train sufficient numbers of staff and managers in IT skills to enable effective implementation of information security measures. Policies must be matched by staff training; and when staff travel to the field they should be comprehensively briefed on the information security procedures they are expected to follow.

6 Interview, 13 October 2009.
7 Interview, 18 December 2009.
8 Interview, 4 January 2010.
9 InterAction 2008:1.
10 Tactical Technology Collective and Front Line Defenders, available at: http://security.ngoinabox.org/ (accessed 20 November 2009).
11 Interview, 29 October 2009.

b. Surveillance

The possibility of becoming the subject of surveillance is particularly challenging for NGOs. This is not a new issue: all manner of actors, from belligerent groups and criminal gangs to intelligence services, have long been cognisant that NGOs are frequently privy to potentially valuable information. Equally they have been aware that NGOs often have access to (even if they do not record) sensitive information regarding their activities, ranging from information on troop dispositions to details of atrocities committed.

Though not new, surveillance is a problem that evolves as technology does. Where a decade ago one might have heard the intelligence officer smoking as he listened in to a telephone call, today it is more likely that a programme's emails are intercepted without staff ever knowing, or being able to prove it.[12] Contemporary surveillance software often relies upon "trigger" words, spoken or written, to filter through telephone calls or emails for pertinent information; or they may target the email addresses or telephone numbers of those organisations or individuals who interest them. A component of each programme's actor mapping and context analysis should therefore focus upon the issue of surveillance: would any actors in the country or locality have the will and the means to place a programme under surveillance? If so, how sophisticated could this be? What forms might it take? The emergence of sophisticated surveillance techniques, however, has not made more traditional methods redundant; actors may continue to use measures such as blackmailing national staff and planting informants as well as, or instead of, more high-tech surveillance means.

The issue of surveillance should not become too dominant, however. It is one aspect of the much wider information management challenge, and, as one interviewee observed, surveillance of NGOs will more often than not lead to proof of innocence rather than guilt.[13] This is not an excuse for taking no information security measures; simply to qualify the problem, and to suggest that information security is not the only bottom-line.

However, an issue of import to every aspect of information management – and especially under conditions of surveillance – is that of **what** an NGO collects, stores, analyses and communicates. If an NGO suspects surveillance reference should be made to its risk threshold. If the information it stores could potentially lead to serious adverse repercussions for its beneficiaries, staff, partners, assets, programmes, donors and/or reputation, should it be stored at all?

Further, NGOs should not expect their mandate alone to convince suspicious actors of their neutrality; they should at all times be conscious of how particular actions (e.g. the subjects and language used in email/phone discussions) could be **perceived** by various actors. One example is that of an agency expelled from a country during the Balkan wars. Its situation reports had recorded the numbers of various types of military hardware spotted on journeys to programmes. It was accused of spying; unbeknownst to it, its communications with headquarters – in a state with which the host-country was at war – were being intercepted.[14] It is thus possible to see how the contextual information communicated was misinterpreted. Shaping perceptions is crucial to acceptance strategies. This applies in the field of information management and surveillance as much as anywhere else.

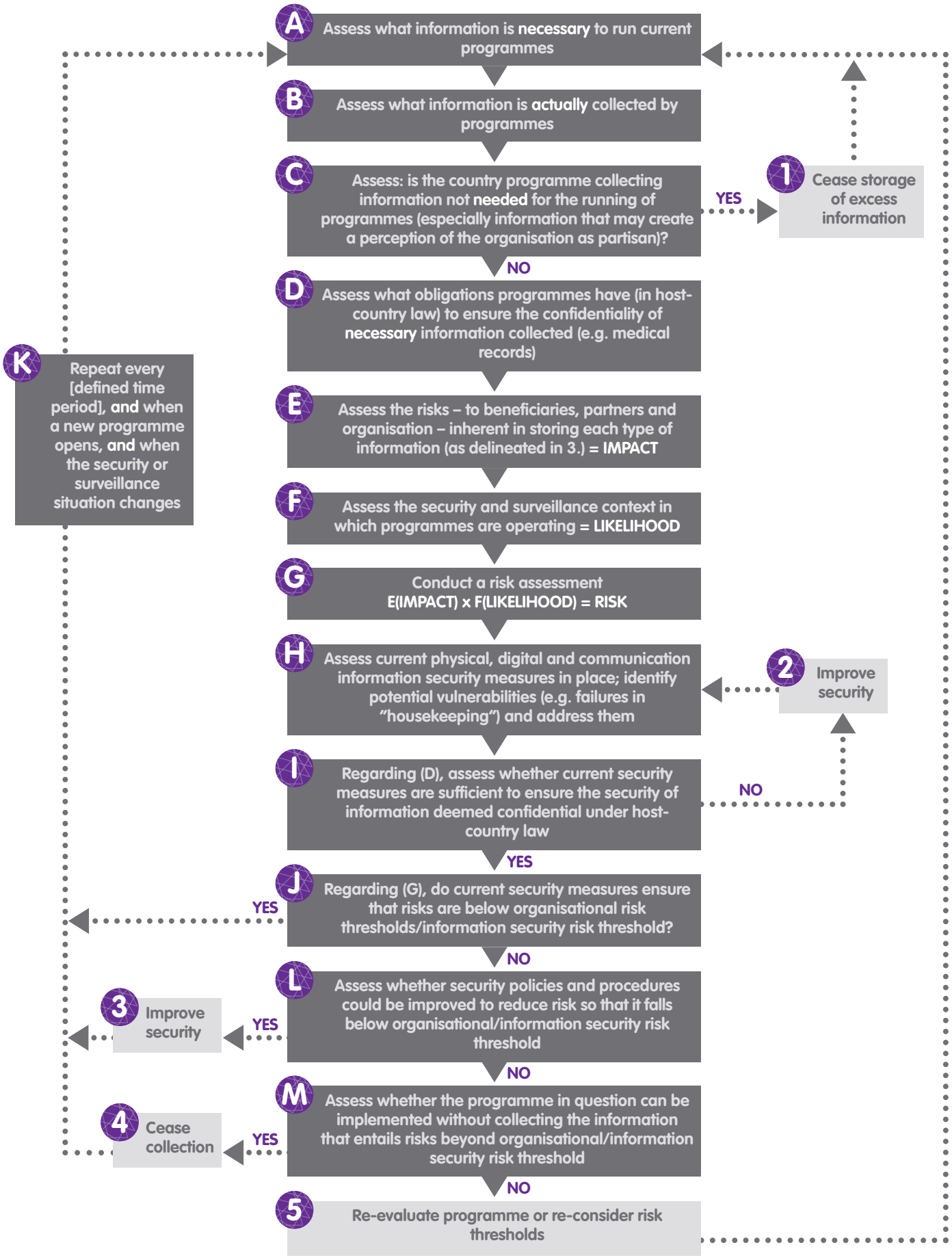
The information management process

The purpose of information management policies is to reduce the risks to beneficiaries, partners, staff and the organisation itself inherent in collecting, recording and communicating information, whilst ensuring that information is still accessible to the right people in a timely fashion.[15] This paper argues that, to be successful, information management policies have to cultivate a process, implemented almost subconsciously in the everyday actions of staff and field operations, integrated into their wider risk management procedures, rather than being a purely technical document.

Below is a suggested framework for the type of process an information management policy should ensure. The procedure moves from identifying the types of sensitive information stored, to the degree of risk inherent in each data set, to the measures currently – and feasibly – taken to ensure their confidentiality. The process key – found in Annex 1 – explains each step.

12 Interview, 12 October 2009.
13 Interview, 27 October 2009.
14 Interview, 12 October 2009.
15 Internal document provided by an NGO, 16 December 2009.

Figure 1 **The information management process framework**



Protecting sensitive information

There are myriad methods of protecting information: this paper divides them (quite artificially) into "physical" and "digital" practices, with a separate section for the complicated issue of "communications". To ensure good information security, all aspects of the problem must be tackled in a holistic fashion; all security measures can be undermined, for instance, by failing to encrypt back-up copies of files and leaving them vulnerable to physical theft. Furthermore, efforts are compromised should good "housekeeping" be ignored.

The sensitivity of the information collected, stored and communicated, and the threats potentially posed by the context, will define the precise strength of security procedures followed. A certain baseline of information security should be observed regardless of context. Interview transcripts for advocacy reports, for instance, should always be confidential, and precautions should be taken to ensure that this is so. However, in more difficult environments, security procedures will necessarily be stronger, more complex and, following that, awkward. In extreme circumstances, an agency may choose **not** to record certain sets of data, deeming the risks they entail simply too high (e.g. beyond stated risk thresholds).

Again, a note of caution is required. Too strict and conspicuously heavy security poses its own risks: it could potentially restrict the operation of life-saving programmes; staff could fail to adhere to it, regarding it as "over-the-top"; or it could raise the issue of "self-incrimination".[16] In the latter case, actors may observe the measures an NGO takes to protect information and assume that it has something to hide. This could prompt surveillance or harassment of staff. Security is in part about balance between being so lax that it is non-existent, and being so secure that self-incrimination occurs.[17]

Key aspects of physical, digital and communications security are identified in Annex 3, which introduces the specific challenges – from securing office spaces to protecting against computer viruses – an information management policy must address.

a. Access levels

One conceptual method of improving security, whilst ensuring that the right people can still access the right information punctually, is to categorise all sensitive information and then determine who requires access to which categories (delineated in section 3) stored by a programme. This will help NGOs to find the correct, context-determined balance between information management's security and accessibility elements. One could divide a programme's staff into different types:

- Line management
- Teams (medical, protection, etc.)
- Departments (logistics, finance, etc.)
- Expatriates
- National staff
- External (other agencies, donors, etc.).

Sensitive information can thus be categorised and individuals' "access levels" to certain categories determined by their position or role. Only the HR department should have access to CVs and salary information; medical records should only be accessible to medics; cashflow information to the finance department, and so on. The greater the potential risk posed by particular types of information, the fewer the categories of staff who should have access.[18]

As a general rule, there may be certain types of information that an agency will choose to restrict the handling of to international staff. National staff are arguably more vulnerable to threats such as pressure or intimidation from armed groups, criminal organisations or repressive governments due the fact that they themselves, and their families, reside in the country in which the programme operates. Thus, to ensure information security it may be necessary to limit their access levels accordingly.[19]

b. Good housekeeping

As an InterAction paper bluntly argues, 'No one can fix stupid. No matter what the technology might be, it doesn't matter if stupid overrides.'[20] Good information security is largely about housekeeping, or what IT specialists sometimes term an aspect of "social

16 Tactical Technology Collective and Front Line Defenders, available at: http://security.ngoinabox.org/ (accessed 20 November 2009).
17 Interview, 26 October 2009.
18 Internal document provided by an NGO, 16 December 2009.
19 Interview, 4 January 2010.
20 InterAction 2008:1.

engineering". Almost any security measure instituted can be circumvented with the inadvertent aid of poor housekeeping. Heavy, expensive locks can be undone by failure to keep track of the number of key sets produced. Anti-virus software is rendered ineffective by failure to keep its virus definitions up-to-date. And a firewall is potentially punctured by a user designing a "weak" password.

Good housekeeping is premised upon awareness, common sense and discipline, combined with and supported by a clearly formulated and communicated policy, creating a continuous, almost subconscious implementation of fundamental security procedures; an "information management culture". Poor housekeeping is arguably the result of the inverse: information management being treated as a purely technical issue, the domain of IT departments alone.

A "culture of security": integrated information and risk management policies

The objective of information management policies is to reduce the risks to beneficiaries, partners, staff and organisations inherent in collecting, recording and communicating information, whilst ensuring that the right individuals have access to the necessary information in a timely fashion. To achieve the highest level of effectiveness information management policies must be tied into wider risk management measures; as integral as the collection, storage and communication of information is to the management and output of programmes themselves.

An information management policy must therefore:

- **Identify** all the information each programme collects
- Facilitate the delineation of **sensitive** information, using the programme's actor mapping, context analysis and risk assessment procedures
- Posit context-determined methods of **protecting** that information, including determining access levels
- **Determine** when information sensitivity outstrips the agency's risk threshold.

An information management policy identifies **what** you store; **how** you should store it; and indeed **whether** you should store it.

It should be fundamentally adaptable, as it will be applied to a range of contexts, from the benign to the high-surveillance. And it should strive to balance the risks of being too lax with security, and being too heavy and inviting self-incrimination or restricting unduly the functioning of programmes. Information management is in part about ensuring that the right people can access the right information at the right time[21]; its security aspect has to be measured against this imperative, and a context-determined equilibrium found. In high-risk areas, the weighting will be toward security; in low-risk areas, toward accessibility.

There is scope therefore in information security policies for the inclusion of a guidelines document, explaining particular security measures that could be taken depending on the severity of risk faced. The security and surveillance situation could be ranked 1-4, with each incremental increase in its severity prescribing additional information security measures to be followed (this is considered in greater detail in Annex 2).

Additionally, information management policies and measures have to be holistic to be effective. They should consider all angles of the challenge – physical, digital, communications, etc. – because vulnerabilities in one area potentially negate security precautions in others. And they must cover every aspect of the information "life cycle", from collection to deletion or destruction.

The policy, whilst having extensive input from IT departments or consultants, should aim to secure "buy-in" from field staff and managers. It should thus be written (or at the very least, extensively reviewed in draft stage) by those who have experience of field conditions. It is staff and managers who will ultimately be relied upon to implement the policy; it must be tailored to their needs, and be clear and concise. Fundamentally, each humanitarian NGO should guarantee that it has sufficient numbers of IT-literate security staff and managers. This has sometimes proven a factor limiting

21 Internal document provided by an NGO, 16 December 2009.

the ability of NGOs to implement their existing information management policies.[22] Information security policies, no matter how clear and coherent, require a core of staff in each programme capable of understanding the complexities of their implementation. And each staff member, on arrival at a programme, should be well-briefed on their information security responsibilities.

Finally, to reiterate, the objective of an information management policy is to inculcate good information management practices into agency and programmatic thinking as a process, seamlessly integrated into wider risk management procedures, rather than as an isolated technical issue. In this way the risks of collecting, recording and transmitting information are reduced, and the right individuals can access information in a timely manner. When this is so, an information management culture has been successfully cultivated. Through the strengthening of such a culture information security policies can become increasingly effective and good housekeeping practices can be consistently observed.

22 Interview, 29 October 2009.

Information Management Process Key

1. Process key

Boxes (A), (B) and (C): identify what information is **necessary** for the agency's current programmes in-country to function, and compare this to the information **actually** collected, stored and communicated. European data protection law stipulates that only information required for the purpose for which it is stored can be recorded regarding individuals. This is a good benchmark to adhere to, and most probably corresponds to host-country law, which is always the first point of reference.

Additionally, collecting only what is **necessary** should eliminate the problem of collecting and communicating information that may appear partisan or ambiguous, and could be perceived as contravening the humanitarian mandate.

Box (D): beneficiaries have a legal right for the information collected about them to be confidential to the standards stipulated by their country's law, and NGOs may feel an ethical duty to ensure that their information security practices also match those imposed by their home-country law. Medical records – no matter how mundane, basic and uncompromising – have access to them strictly regulated in most states' laws and in Europe. Failure to meet the strictures of relevant law could result in legal redress for staff or organisations.

Boxes (E), (F) and (G): these boxes denote a risk assessment, with each category of information identified in (B) given a "risk", based upon the potential **impact** of its being accessed unauthorised and the **likelihood** of this occurring. Clearly, to assess risk accurately, this process has to be embedded in the programme's actor mapping and context analysis measures.

Surveillance is an aspect of this, and a humanitarian NGO has formulated a four-level surveillance scale:

1. Agency is expected to be expelled from country imminently
2. Agency is subject to active and aggressive monitoring by state agencies
3. Agency is subject to active/passive and non-aggressive monitoring by state agencies
4. Agency is subject to monitoring by third parties (non-government).[1]

If under surveillance, quantifying this monitoring will allow the "risk" of storing particular data sets to be accurately determined.

Box (H): assess the physical, digital and communication security measures currently in place. If obvious gaps – e.g. failures in "housekeeping" – are identified, they should be closed immediately.

Box (I): are the programme's existing information management practices consistent with the organisation's obligations regarding (D)? For instance, does the programme restrict access to medical records in accordance with host-country laws? If not, serious consideration should be given to improving security measures until this is the case. This could include strengthening the "technical" measures in place, or defining access levels (see section 6.A.) more tightly. Again, issues of legal liability flow from failure to implement procedures conforming to local law.

1 Document provided by an EISF member, released17 August 2009.

Box (J): the "risk" inherent in collecting, storing and communicating each category of information, identified in (G), should be measured against the agency's organisational risk threshold, or information security specific risk threshold. The risks to the organisation in question, its staff, partners and beneficiaries need to be separately measured against this scale.

Box (L): if a particular risk exceeds the risk threshold, the degree to which this risk could be reduced by implementing more stringent information security measures, thus limiting the likelihood of an information breach occurring, needs to be assessed.

Box (M): if improved security measures cannot reduce the risk sufficiently to press it below the organisational/information security risk threshold, thought needs to be given to either: reshaping the programme so that the offending information is no longer collected; or to discontinuing the programme. If the programme is judged critical, the risk threshold could be adjusted with caution, so that incremental rises in the threshold do not result in "risk creep" and render the threshold meaningless.

Box (K): information management is continuous. To be effective, a culture, based on a constant awareness of the issues concerned, must be cultivated. A process of this kind thus should be repeated at specified intervals and according to the given indicators. Even more than this, the basics of information security – the good "housekeeping" central to rendering it effective – should be internalised by all staff members.

Anatomy of an Information Management Policy

1. Introduction and purpose

The information management policy should describe its ultimate purpose: to integrate information management and security into organisational and programmatic thinking as a process, if necessary instilling a change management process that strengthens the organisational "information management culture".

2. Responsibilities

The document must delineate responsibilities for ensuring that information management is successfully integrated into agency and programmatic thinking. A suggested division of responsibilities is:

- The organisational Head of IT in headquarters frames the technical policy, including a 1-4 ranking of security measures to be followed depending on the severity of the security situation (explained in 5 below). He/she is also responsible for ensuring that the policy is updated when necessary. In smaller organisations, independent consultants could fulfil this role. It is also HoIT's, and Human Resource's, role (in the latter case, through recruitment criteria) to ensure that the organisation has enough IT-trained staff/managers to implement the policy. A field-experienced manager must be allocated the responsibility to co-draft, or extensively review, the policy so that it is realistic and appropriate to field conditions.
- At country programme level, a Chief Information Officer (CIO) or equivalent, or the Security Focal Point (SFP) or a line manager, is given primary responsibility for ensuring that the organisation-wide policy is implemented in their programme, and that security procedures are consistent with the security/surveillance context. He /she must ensure that regular, routine audits of information management practices are undertaken (see 6); that audits are undertaken after "trigger" events (e.g. a change in the surveillance context or opening of a new programme); that access levels are determined; that new staff are briefed on their responsibilities on arrival and that they sign the relevant acknowledgement forms (see 8).
- Line managers are responsible for ensuring that their teams/departments implement information security procedures relevant to them.
- Staff are responsible for ensuring constant implementation of the general security measures as well as specific measures relevant to their role, such as locking doors and windows at night, not opening email attachments from unknown sources, ensuring medical records are protected as mandated by the CIO/SFP/line manager, etc.

3. Risk management

The document must facilitate the identification of "sensitive" information. It should thus define "sensitive" information, and then outline a process designed to identify when data collected by a programme matches this standard. This can be done most effectively when incorporating information management and security into wider risk management processes, including context analysis, risk assessments and risk thresholds.

The document must either stress that the risks each data set carries must be measured against the agency's overall risk threshold, or define a risk threshold specific to information management. The policy should also identify a process to determine what happens next should data vital for the running of a programme exceed the risk threshold.

4. Baseline security measures

The information management policy must describe a baseline level of information security that should be followed regardless of context: for instance, "strong" passwords should always be used; anti-virus software must always be installed and its virus definitions kept up-to-date; the office always kept secure, with the number of key sets produced, and their locations, always tracked.

It should ensure that staff are appropriately oriented and trained; and that sufficient resources are allocated to enable the implementation of security measures (e.g. funds are set aside to renew anti-virus software licenses, to purchase lockable cupboards, etc.). If new offices are to be opened, it should propose criteria for selecting the office site and ensuring that it is as secure as possible.

Subheadings could include:

- System access (defining who has, and under what circumstances, access to the agency's computer systems)
- Physical security (including of hard copies)
- Internet and email security
- Blogs and social networking
- Computer viruses and spyware
- Backing-up
- Landline, mobile and satellite telephones
- Destroying information

Each of these will describe the relevant security measures the programme should follow as a minimum. Further details on each aspect can be found in Annex 3.

5. High-risk or surveillance environments

The information management policy could also outline precautions that should be taken in high-risk environments (e.g. those with high levels of political violence and/or crime) and when under surveillance.

One method of addressing this issue is quantifying the security/surveillance environment into four levels. Each level would have associated information security procedures that would have to be followed under each of the subheadings above (section 4), and would impose certain demands upon staff orientation and training procedures, and outline budgetary requirements for implementing tighter security procedures.

Level 1, the lowest level of danger, would require only that the baseline security procedures are followed (see section 4 above).

Level 2 would denote a medium- to high-risk country in which surveillance was not suspected. It could entail tighter restrictions on what type of information is stored, more frequent auditing of security measures, more frequent mandatory changes of important passwords, etc.

Level 3 could describe security measures in medium- to high-risk countries where surveillance is suspected, and would require programmes to implement wider use of encryption software (if legal, and if it is determined that this will not exacerbate the surveillance problem through self-incrimination), and impose more stringent limits on the volumes and types of information stored and communicated.

Level 4, in which the security situation was serious, sophisticated surveillance was apparent, and the agency was expecting to have to evacuate or to be expelled in the near-term, would seriously limit the volume and types of information stored and would require the agency to follow very strict security procedures, and prepare for destroying information.

6. Auditing

The document must outline what measures will be used to periodically internally evaluate each programme's information security practices, and how often this process will take place (every month, quarter, etc.). Because information management is integral to successful security and risk management, such audits could, or perhaps should, be a component of general security audits or reviews. The audit must determine:

- The degree to which existing policies are implemented
- Their adequacy compared to the risks the security/surveillance context poses
- If staff orientation/training measures are appropriate and sufficient for the security context
- If information security measures are adequately resourced.

A salient element of the auditing process will be repeating context analysis and risk assessments to

identify whether the security/surveillance situation has changed (e.g. it has become less permissive); if so, the degree of "sensitivity" of information will change also and this needs to be assessed. This will determine whether the security, training and budgetary measures in place need tightening or increasing (or, if the context becomes more permissive, vice versa).

The document must also outline "triggers" for an information security audit, such as a tangible change in the security/surveillance situation, or when a new programme (requiring the storage of new information) is opened.

The audit section thus has to emphasize the continuous nature of information security, leading to its ingraining as a process rather than a one-off event.

7. Violations

The policy must outline the sanctions that will follow certain violations of its strictures. These can come in two forms: "internal" and "external". Internal sanctions refer to those the NGO in question reserves the right to use against staff who fail to follow procedures outlined by the information management policy (e.g. by opening suspicious email attachments, or visiting prohibited websites).

External sanctions refer to formalised means outside actors can use to seek legal redress for transgressions of relevant information security or data protection laws. Should organisations or staff fail to uphold relevant data protection laws, either through deficient procedures, poor implementation or negligence, the organisation or staff could be liable to litigation.

8. Acknowledgement forms

An information security policy should require staff to familiarise themselves with:

- The policy itself
- Their obligations under host-country data protection legislation
- The conclusions of the programme's contextual analysis procedures regarding information security and the risks they should be aware of
- Their responsibilities, including the security procedures that they must implement in their daily routine (see section 2 above)
- The organisation's information systems code of conduct.

Specific "acknowledgement forms" should be composed, with staff signing them once they are confident that they have been effectively briefed on their responsibilities, and have read and understood the relevant documents.

Key Aspects of Physical, Digital and Communications Security

Annex 3 seeks to elucidate the precise vulnerabilities in physical, digital and communications security that an information management and security policy should address.

1. Physical Security

Physical security is the protection of computer hardware, office facilities and organisational assets from physical circumstances and events that could cause serious damage or loss, including theft, fire, and natural disasters.[1] It is in part about common sense, but it is no less valuable for its apparent simplicity. One could install every relevant type of information security program, from anti-virus to encryption software, but it would prove of little use should a computer be stolen by an intruder who unlocked a door using a set of keys no one had realised was lost, or if it is destroyed in a natural disaster.

The basics of physical security, and the issues one has to consider in each particular context, are thus:

The office

A thorough assessment of each office space a programme uses should be conducted. Access to the office and the various spaces inside it will be a fundamental issue. Questions that should be asked include:

- How secure are the locks on both doors and windows?
- How many sets of keys have been produced and is there a system in place to keep track of them?
- Are locks replaced if a key goes missing (especially in suspicious circumstances)?
- Are all doors/windows locked securely when the office is empty?[2]

Additionally, if possible, visitors to the office must be restricted from accessing the main workspaces. Each office should have a reception or waiting room area so that visitors cannot eavesdrop upon conversations or telephone calls, or view employees' computer screens, whilst they wait for appointments.

When printing or faxing, potential vulnerabilities must be addressed:

- When sensitive documents are printed they should be retrieved quickly so as to prevent them being examined or taken
- If a fax containing sensitive information is expected, a time should be agreed for its receipt so that it can be collected immediately
- Printers and faxes should be disconnected and shut down at the end of each day, thus wiping their local memory (this is model-dependent, however).[3]

A number of simple policies can be used to further protect hardware and information:

- Security cables should be used to lock laptops to desks to prevent theft
- A "clear desk" policy should be observed, so that at night no documents are left on work spaces but are instead locked away in secure filing cabinets
- It should be standard practice for users to "screenlock" computers when they leave their desks, even for brief periods

1 Search Security.com, available at: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1150976,00.html# (accessed 20 November 2009).
2 Tactical Technology Collective and Front Line Defenders, available at: http://security.ngoinabox.org/chapter-2 (accessed 20 November 2009).
3 Internal document provided by an NGO, 17 August 2009.

- Locked cupboards should be used to store laptops and USBs when not in use
- Wireless routers and servers must also be placed in locked (but ventilated) spaces. Both are otherwise vulnerable to having malicious software installed on them that can intercept the information they transmit and process.

Finally, the area surrounding the office is clearly of import regarding its security. Are those living nearby potential allies or threats?[4] If intrusion is considered a particular risk, installing a surveillance camera may act as a useful deterrent.

Travelling

When travelling, laptops, phones, cameras and other electronic devices (such as CDs and USBs) must be kept on the individual's person at all times, including meals (when thieves often target hotel rooms, secure in the knowledge that the occupant is unlikely to be in), though expensive electronic devices should not be prominently displayed or "shown off". When travelling from head office, "clean" laptops, USBs, phones and cameras should be taken so that loss (or their seizure at customs, for instance) does not compromise potentially sensitive information.[5] It is important also to protect the information collected on a trip, perhaps using file and/or disk encryption (see section 2 for further details).

Surveillance

If surveillance is suspected, simple measures may reduce the risk; though clearly what is collected, stored and communicated is of central concern in this context. Background noise – music or the radio – can be used to run the battery down on "bugs" or disrupt remote microphones. Drawing curtains can prevent physical observation of an office or computer screens, and also reduces the vibrations of the window (which can be used to eavesdrop upon conversations using sophisticated microphones).[6] Sensitive face-to-face conversations can occur in outside areas with background noise.

Destruction

Computer hardware and the information stored upon it should be protected from destruction caused by fire, irregular power supplies and natural disaster as well as from deliberate theft.

An information management policy should thus mandate programmes to take measures to reduce the chances of hardware and information destruction or loss. For instance, in countries whose power grids are prone to power surges and blackouts, Uninterruptible Power Supplies (UPS) should be used to prevent sudden power surges or losses "crashing" hard drives and corrupting files held on them.[7] And basic precautions against fire, such as not connecting too many appliances to single plugs using multi-plugs, should be explained.

2.Digital Security

Digital security is the protection of electronic files stored on computer devices – from mobile phones and PDAs to USBs and computers – from unauthorised access, corruption, loss, misuse or destruction.[8]

Basic digital security measures should always be observed, such as password-protecting user accounts, wireless internet networks, and sensitive documents.

Passwords

An information management policy must:

- Outline the criteria defining "strong" passwords
- Outline the frequency with which passwords, especially those quite commonly known (e.g. for the office's wireless internet network), should be changed
- Ensure that staff are aware of their responsibility to keep passwords (especially those for individual profiles, etc.) secure by stipulating that only the relevant individual(s) (most often only a single person) know them
- Ensure that staff use unique passwords for different purposes, so that the discovery of one does not allow an actor access to every password-protected profile or website the individual uses.[9]

Passwords are crucial to information security; poor passwords, or widely-known passwords, can short-cut most other information security measures.

Hackers and malware

Three of the primary risks flowing from use of the internet are hacking, spyware and viruses. Hacking and spyware seek to gain illegal access to information stored on computer systems; viruses more often to

4 Tactical Technology Collective and Front Line Defenders, available at: http://security.ngoinabox.org/chapter-2 (accessed 20 November 2009).
5 Safer Access 2008:16.
6 Internal document provided by an NGO, 17 August 2009.
7 Tactical Technology Collective and Front Line Defenders, available at: http://security.ngoinabox.org/chapter-2 (accessed 20 November 2009).
8 Business Dictionary.com, available at: http://www.businessdictionary.com/definition/information-security.html, (accessed 20 November 2009).
9 Internal document provided by an NGO, 25 February 2009.

destroy, damage or corrupt it. Tackling these threats requires that installed on computer systems are: a firewall, which acts as a guard protecting computers against unauthorised access from the internet; and anti-spyware and -virus software. The information security policy must ensure that:

- Anti-spyware and anti-virus software are kept up-to-date to protect against new threats
- Opening email attachments – a common method of viruses and "Trojan" hacking software gaining access to systems – is strictly regulated so that attachments from unknown sources, or ones that are not trusted, are not opened[10]
- Wireless internet networks are password-protected, with the password changed regularly if widely known.

Encryption of files and disks

Perhaps the most powerful tool for protecting recorded sensitive information is encryption of files and disks/USBs. Encryption codes information with formulas rendering it unreadable by anyone without the specific "encryption key". An information management policy should thus posit criteria determining when and where encryption software should be used to protect sensitive information.

Though powerful, it is wise to be aware of the risks associated with encryption's use. Encryption is only as strong as its weakest link; frequently this is the password used to access secure files or encrypted volumes.

Encryption could also, if the relevant password is lost, lead to programmes being unable to access files vital to their operation, resulting in programme interruption. Potentially just as costly is the problem of "self-incrimination". Before travelling, and before installing encryption software, the legality or otherwise of encrypting files or hard disks in the destination country should be ascertained (it is illegal in some countries). Even where encryption is legal, the risk of self-incrimination may still be present: actors could perceive an organisation's use of encryption as tacit acceptance that it has something to hide, and it could hence prompt suspicion, surveillance or harassment.[11]

Despite the risks associated with it, encryption is a very effective method for protecting sensitive files and disks. Encrypted files potentially require very powerful computers to crack. Additionally, there are methods available to reduce the risk of self-incrimination. Most simply, encrypted files or folders can be hidden amongst reams of routine information: "security by obscurity". Alternatively, some types of encryption software have the capability to create "hidden volumes"; what appears to be a single encrypted folder will be two. One could be filled with convincing, semi-sensitive files (e.g. out of date financial details); the other with genuinely sensitive information that the agency wishes to protect. Which folder is opened depends on which of two passwords is used. Thus, if an employee comes under pressure to open the encrypted volume, he/she can reveal only the "decoy" password leading to the first volume, potentially convincing the malicious actor that the NGO is only protecting information of no interest to it. This offers "plausible deniability".[12]

One important caveat should be reiterated at this juncture. Encryption is a powerful tool, but there is no such thing as "one-hundred percent security". Encryption software can be cracked with time and (very) powerful computers, or pressure and intimidation can be used by actors to force staff to reveal passwords to "hidden volumes".

Access levels

As discussed in the main paper information and staff can be categorised, with certain information only accessible to staff in relevant roles or of sufficient seniority. To ensure that this is the case, documents can be password-protected or encrypted, with only the relevant staff having the password to particular categories of a document; or each department or team could have its own shared drive, with files only relevant to their group saved on this drive and thus only accessible to those with computer profiles linked to it.

As noted in the main paper, and especially in high-risk areas, certain sensitive types of information could have access levels determined so that only international staff can handle them. This is because national staff are potentially more vulnerable to threats and intimidation compelling them to disclose information to outside actors unauthorised.[13]

3.Backing up

Risks of hardware damage or loss can never be completely eliminated. Central to an information

10 Tactical Technology Collective and Front Line Defenders, available at: http://security.ngoinabox.org/chapter-1 (accessed 20 November 2009).
11 Ibid., http://security.ngoinabox.org/chapter-4 (accessed 20 November 2009).
12 Ibid., http://security.ngoinabox.org/chapter_4_2 (accessed 20 November 2009).
13 Interview, 4 January 2010.

management policy must be guidelines on how, and how frequently, to back-up files, ensuring that programme interruption is kept to a minimum in case of disaster.

Backing-up requires that programmes first identify the location and method of storage of all the information they record (e.g. files on programme **A** are stored on computer **X** in office **B**, or on USB **Y** in possession of employee **C**), including duplicates, and then define a method of creating regularly-updated second copies of each file. These copies must be kept in a separate location to the original; otherwise a flood, for instance, could wipe out both.[14] So that backing-up becomes routine, an information management policy should mandate that programmes back-up at defined, regular intervals (e.g. every evening, or every Wednesday evening). It should ensure that responsibility for backing-up is clearly delineated, and that a secure site for storage is carefully selected. The more regularly and routinely backing-up is performed, the greater the chance that data loss, and programme interruption, will be minimal.

Digitising information – rather than storing it as paper files – potentially greatly increases the speed and ease of backing-up; it is much easier to duplicate files onto a CD, and to physically transport that to a separate location, than it is to do the same with hundreds of pages of paper. Finally, backed-up files should be encrypted (if legal in the country concerned); otherwise a malicious actor could gain access to everything the programme has stored solely by, for instance, breaking into the location in which the back-ups are stored.

4. Destroying information

An information management policy should also articulate clear guidelines on how and when information is to be destroyed. The policy should be formulated with the provision in mind that this may have to be done quickly. In Sudan, for instance, many NGOs operating in Darfur were expelled at short notice, compelling them to destroy the sensitive information they had amassed during their programmes. This process was largely unplanned for and ad hoc, however, and thus proved conspicuous. It subsequently aroused the attention of the already suspicious Sudanese authorities, who arrested several aid workers in order to determine what NGOs had been destroying.

In high-threat environments, especially those in which sophisticated surveillance is suspected, certain types of information – entailing levels of risk to the agency, its staff or beneficiaries that exceed its organisational risk threshold – possibly should not be collected and recorded. Additionally, sensitive information should be clearly delineated (to staff) from routine information. Thus, should a programme's deteriorating context mandate a rapid destruction of sensitive information, it will prove possible to rapidly identify what needs destroying, and when this process is complete.

Digitising information – rather than storing it in paper form – could also increase the speed and ease of destroying information. Destroying a few hard drives is a much quicker process than shredding thousands of pages of paper.

To destroy information so that it is impossible (or nearly impossible) to recover:

- Paper documents, CDs/DVDs, floppy disks and mobile phone/PDA SIM cards should all be shredded (using a "cross-cut" shredder)
- Hard drives should be erased using computer programs designed to do this securely, though these programs can take some time (often between five and fifteen hours)
- If in a rush, hard disks (whether for computers or PDAs) can be physically destroyed by driving a nail through them.[15]

5. Communications security

Information is perhaps at its most vulnerable when being communicated. Most radios used by NGOs are not secure, telephone calls can be bugged, emails intercepted, and so on. As with all information management, there is no perfect solution. An information management policy therefore should identify how to communicate in particular environments, from the benign to the high-surveillance.

An issue is thus what you communicate. In circumstances where sophisticated surveillance is credibly suspected, it may be best simply to avoid engaging in certain, potentially very sensitive, conversations – for instance, regarding advocacy strategies – over email or telephones, or to at the very least minimise the exposure of sensitive information.

14 Tactical Technology Collective and Front Line Defenders, available at: http://security.ngoinabox.org/chapter-4 (accessed 20 November 2009).
15 Interview, 30 November 2009.

Perhaps the most challenging aspect of communication is determining how to commence and maintain secure communication. If travelling to an area in which surveillance is suspected, it is thus sensible to agree before leaving on how communication will be sustained (e.g. through email, VoIP?), whether to use a code system, whether encryption will be used and so on. This will avoid having this potentially compromising discussion under the noses and possible observation of malicious or suspicious actors.[16]

One method of transmitting sensitive information even where surveillance is suspected is splitting information over various means of communication. If, for instance, targeted attack is a high risk, one could use satellite phones to outline the locations staff will visit and email to provide the times they will visit each (using codes as a further layer of protection).[17]

Finally, both email inboxes, sent items, etc. and memories of PDAs and mobile phones should be regularly emptied (and saved exclusively in back-ups, if necessary) and contact addresses/numbers of sensitive interlocutors held in code.

Radios

Most radios used by NGOs are not secure. By tuning into the same frequency being used, any individual can listen to conversations taking place. Thus, an information management policy must ensure the use of codes – using alternate names for places, people and equipment – whilst identifying the potential weaknesses of this; no code is unbreakable, especially if the observer has "inside" help. It should also mandate the use of strict radio discipline, so that exposure of sensitive information is kept to an absolute minimum.[18]

Telephones and Voice over Internet Protocol (VoIP)

Landlines, mobile or satellite telephones are never completely secure, and it is often very difficult to determine whether conversations are being intercepted. Telephone, mobile (including text messages) and VoIP conversations can be scanned for "trigger" words, or telephone numbers or IP addresses observed. Court orders can be used to force mobile phone networks or Internet Service Providers to reveal numbers called from various phones or websites visited from particular IP addresses. Satellite phones are perhaps the most secure, but even their communications can be monitored. Means such as purchasing several local SIM cards (preferably at separate locations and on different networks) can increase individuals' anonymity, especially if they discard SIM cards after using them for short periods. Mobile phones can be purchased that have built-in encryption technology, but both caller and receiver need to have the same type of phone/encryption software for this to function, and it raises the issue of self-incrimination.

Skype claims to be secure, and it uses a very high level of encryption technology, but there are exceptions to its professed standards. In China, for instance, the only version of the software downloadable in the country (TOM-Skype) has a filter that scans text messages and sends those with "trigger" words to a central (government-controlled) server.[19] Skype also shares information extensively and openly with the US government. It is not impossible that more such "exceptions" exist than are currently known about, or that more may occur in future. Thus, Skype is to be considered an insecure means of communication, especially where surveillance by the local government is suspected.[20]

Email

Email is subject to different levels of vulnerability depending on what program or provider is used. Gmail is the most secure well-known webmail provider, for instance, in that it encrypts each user's username/password and the text of each message (if one types "https" rather than "http" at the beginning of the web address), whilst Yahoo and Hotmail only encrypt the former. Many webmail providers, however, expressly prohibit organisational usage in their Terms of Use, and access to the information each account contains can be granted through court orders (and the provider is then under no obligation – and sometimes is expressly prohibited – from notifying the account holder). As Google's recent spat with China also illustrates (over China's alleged hacking into the accounts of Chinese human rights advocates), state authorities are rarely above monitoring the accounts of those individuals or groups they regard as suspicious.[21]

Basic procedures can strengthen email security, however. Using a code when sending sensitive information can reduce the exposure of sensitive information and avoid the use of "trigger" words; and strong, frequently-changed passwords are crucial.

If one suspects that institutional email addresses are

16 Ibid.
17 Internal document provided by an NGO, 16 December 2009.
18 Internal document provided by an NGO, 17 August 2009.
19 Interview, 30 November 2009.
20 Internal document provided by an NGO, 17 August 2009.
21 See, for instance, http://news.bbc.co.uk/1/hi/8455712.stm (accessed 23 February 2010).

being monitored, opening a webmail (e.g. Gmail) account in an internet café (so that the account is not tracked to the IP addresses of agency computers) could provide an extra means of transmitting sensitive information that malicious actors may not be aware of.

Also, emails should never contain both sensitive and routine information; only one or the other. Otherwise the recipient may fail to distinguish between the two and share and store sensitive information as if it were routine.[22]

Email communications are only ever as secure as their recipient(s).[23] If the recipients do not use secure (e.g. encrypted) email accounts; if they fail to log out correctly when they leave an internet café; if they forward messages to others the sender does not know or trust, then the information is vulnerable no matter what measures one half of the conversation takes to ensure its security.

Before sending an email, or making a phone call, several questions should be asked:

- Is it necessary?
- Does it contain any information that could put others at risk?
- Could it foster or reinforce a perception of the sender and their agency as partisan?
- Is the email being sent to only those who need to receive it?
- Should the "bcc" function be used so that each recipient cannot see the addresses of the others?[24]

The answers to these questions determine **whether** the communication should be sent or made and, if so, what precautions should be taken to ensure its security and confidentiality.

Blogs/social networking

An information management policy should have guidelines outlining employees' use of blogs or social networking. Blogs, even if anonymous, can be attributed to a particular user or organisation (either by tracking the website addresses visited by particular computers or by cross-referencing blog contents to individual/organisational activities). Hence it is important to ensure that their content, if associated with a particular organisation, would not adversely affect its security or damage its relationships with particular actors.

Similar caution should be taken when using social networking sites, such as Facebook. Any information that could prove compromising or sensitive to the individual or the organisation for whom they work in the relevant context probably should not be posted on Facebook or similar websites.[25]

Intranet

Most organisations use an intranet within their HQs; this may be accessible in country programmes, or they may have separate intranets. What is stored on these networks, and how accessible the information is, could have implications for information security. If intranets are hacked into, information as minor as work mobile phone numbers could be used to harass staff. And information such as staff profiles could prove compromising. In Darfur, for instance, securing visas for security focal points often involved a degree of obfuscation.[26] Security focal points would often be termed "safety" managers, and their CVs reworked to de-emphasize the security aspects of their careers. Caution as to what is put on the intranet, and awareness of its potential targeting for hacking (especially if passwords to it are fairly freely distributed), should be used.

6. Staff HR practices

The hiring, employment and removal of staff has potential implications for information security. In Darfur, for example, NGOs were compelled to accept government officials observing every interview for new staff, with the likelihood that the national selected would be pressured to inform on the activities of the NGO.[27] Awareness of such practices, and the risks posed to security, is crucial to an accurate risk assessment leading to appropriate information management practices.

Additionally, if a staff member is disgruntled, shortly to be made redundant or has been fired, the information security implications must be considered. A high percentage of information security issues flow from "internal" risks, including the deliberate destruction or distribution of sensitive information.[28] Thus, if a staff member may have a grievance with the organisation, restricting their access to computer systems should be considered.

22 Internal document provided by an NGO, 16 December 2009.
23 Internal document provided by an NGO, 25 February 2009.
24 Internal document provided by an NGO, released17 August 2009.
25 CIO Council 2009:6.
26 Interview, 29 October 2009.
27 Interview, 12 October 2009.
28 Interview, 15 December 2009.

7. Information management is holistic

Delineating information management into "physical", "digital" and "communications" elements is necessary but also rather false. The three aspects fit seamlessly together, with most security risks and matching precautions failing to reside exclusively in any one, or even two, of the categories. For instance, the issue of backing-up crosses all three categories, protecting as it does against programme interruption caused by a range of risks, such as physical loss of computer hardware or the corruption of files by a virus.

That the information management challenge is engaged with holistically – with its physical, digital and communications elements considered as seamlessly as possible, and the information "life cycle", from collection to destruction, envisioned – is hence central to ensuring that the resultant policy is as effective as practicable.

Annex 4

1. Further reading

Security in-a-box – Tactical Technology Collective and Front Line Defenders

http://security.ngoinabox.org/

Security in-a-box is a resource designed for Human Rights Defenders facing risks such as surveillance or pressure to cease their work. It provides guides on how to protect computers from viruses, malware, and hacking; how to ensure the physical security of office spaces; how to create strong passwords; how, and whether, to use encryption software; how to recover from information loss and destroy sensitive information; and how to keep internet communications private.

Laptop Security for Aid Workers – Safer Access

http://www.saferaccess.org/documents/sa_security_of_laptops.pdf

This document provides advice on choosing laptops appropriate to job roles, and basic guidelines on physical and digital security for protecting them and the information they hold whilst travelling or in the field.

Guidelines for Secure Use of Social Media by Federal Departments and Agencies – CIO Council

http://www.fbiic.gov/public/2009/sep/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

This guidelines document is written for the US government and yet its description of the benefits and risks of using social media and networking sites are in part appropriate to the needs and risks of NGOs.

Information Technology – Aid Workers' Network

http://www.aidworkers.net/?q=advice/information_technology

This basic guide to information technology use in programmes provides introductions to free, open-source software and links to other useful information technology and security sources.

TechSoup – the Technology Place for Nonprofits – Techsoup.org

http://home.techsoup.org/pages/default.aspx?cg=lnav

TechSoup works with corporate donors in order to supply NGOs and other nonprofits with up-to-date IT software.

Crypto-Gram – Bruce Schneier

Subscribe here: **http://www.schneier.com/crypto-gram.html**

Crypto-Gram is a monthly newsletter that provides comment on security issues, with a focus on IT security, written by author, op-ed contributor, and British Telecom Chief Security Technology Officer Bruce Schneier.

Safe Travels for You and Your Data – The New York Times

http://www.nytimes.com/2010/02/18/technology/personaltech/18basics.html?8dpces

A short guide outlining precautions that should be taken when using public computers (e.g. in an internet café or library); public Wi-Fi; and your laptop and smartphone/PDA abroad.

2. Bibliography

This briefing paper is based largely on interviews and internal documents provided by EISF members and staff from other NGOs, as well as discussions held at various NGO fora. Below is a list of resources cited in the text, which readers may wish to refer to.

Aid Workers' Network. Information Technology available at: **http://www.aidworkers.net/?q=advice/information_technology [accessed 15 February 2010].**

CIO Council, 2009. Guidelines for the Secure Use of Social Media by Federal Departments and Agencies. September, US Federal Government.

Currion, Paul, 2006. Information Technology Requirements Initiaitive – Assessment Report: Darfur Reponse. In **Emergency Capacity Building Project: A Collaborative Effort of the Inter-Agency Working Group on Emergency Capacity.** Bill and Melinda Gates Foundation.

Currion, Paul, 2006. Information Technology and Requirements Initiaitve – Assessment Report: Findings and Recommendations. In **Emergency Capacity Building Project: A Collaborative Effort of the Inter-Agency Working Group on Emergency Capacity.** Bill and Melinda Gates Foundation.

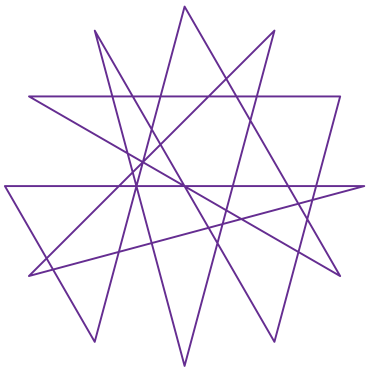
Currion, Paul, 2006. Information Technology and Requirements Initiative – Assessment Report: Global Response. In **Emergency Capacity Building Project: A Collaborative Effort of the Inter-Agency Working Group on Emergency Capacity.** Bill and Melinda Gates Foundation.

InterAction, 2008. Report of Information Security Workshop. May.

Vitaliev, Dmitri, 2009. Cyber Security for International Aid Agencies: A Primer. December, Security Management Initiative.

World Health Organisation, 2002. Medical Records Manual: A Guide for Developing Countries. World Health Organisation.

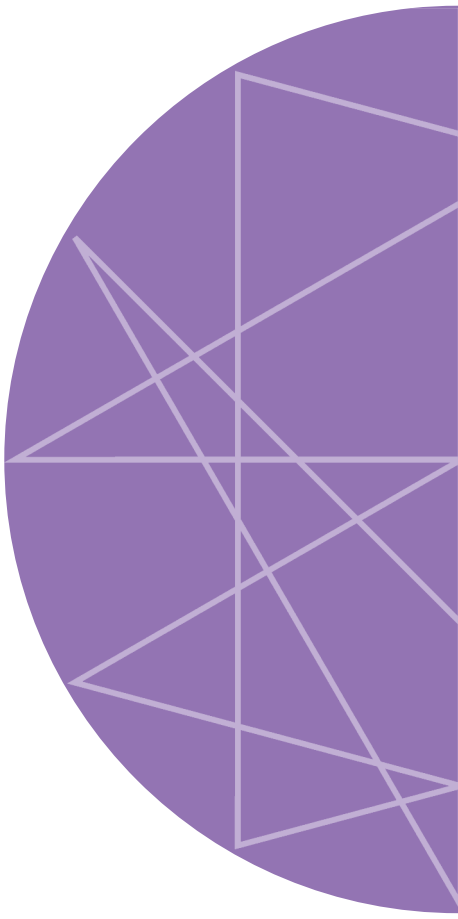
eisf



European Interagency Security Forum
c/o Save the Children
1 St John's Lane
London EC1M 4AR

EISF Coordinator
+44 (0) 207 012 6602
eisf-coordinator@eisf.eu

EISF Researcher
+44 (0)207 012 6726
eisf-reseach@eisf.eu



www.eisf.eu

design and artwork: www.wave.coop