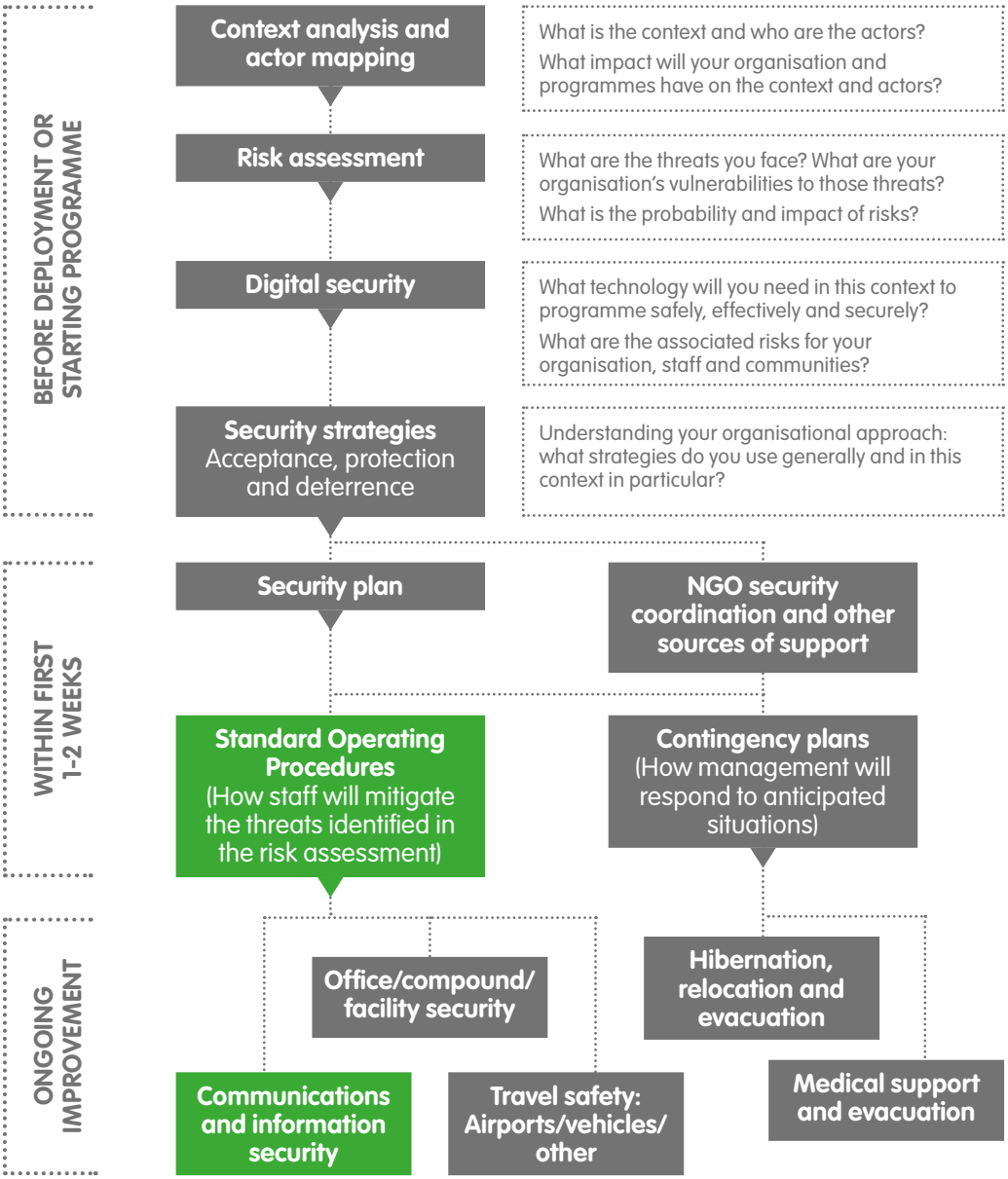
9 Communications and information security



In setting up any new deployment, project or mission, time must be taken to consider what types of communications will be available (landline, mobile networks, satphones, internet, surface mail, courier, etc.) and how reliable they are likely to be. In the modern world, communications are as much a key 'survival' need as food, water and shelter.

Budgeting early for reliable communications systems – including back up and alternate systems for replacing damaged, lost or stolen equipment – is a key component of both staff safety and programme success. Also, some forms of communications such as radios or satellite systems may require licences to operate. The United Nations may be able to give support in obtaining licences. The organisation should budget for airtime and/or licencing where necessary.

Be aware of new technologies that can cost effectively improve your communications such as satellite 'back-packs' for smart phones or satellite messaging systems rather than traditional voice phones. Buy the best you can afford.

However, organisations need to consider the image their communications equipment conveys. If having a low profile is part of the security strategy, adding HF radios and aerials to vehicles will make them stand out as much as a logo.

In regions of conflict, civil unrest or after natural disasters, never assume the internet and mobile networks will be reliable. During security emergencies or natural disasters, governments often take control of (or shut down) networks – at the time you will need them most. It is important to never rely only on a single system whether it is landline, mobile networks, satellite phones, the internet or others.

Be creative. In emergencies, NGOs have used relays of taxi drivers to maintain communications with staff when phones or the internet were down, or used camels to carry messages and maintain contact with remote communities.

Communications security and procedures

Establishing and maintaining an extensive communications network is key to safety, security and success of operations. If you have radio networks or satellite phones, train staff in their use as part of their induction and inform them about where the installed communications equipment can be used (e.g. do you need to be outside? Are there black spots?). Ensure attention is devoted to staff being able to communicate with family and friends during deployments, and especially in emergencies.

A growing number of organisations and coordination bodies are using WhatsApp and other similar social apps for sharing information directly between staff. This can bring great advantages for sharing information in real time, however information in these networks is unverified. There should be clear guidelines on what information can or cannot be shared, and the procedures to follow for acting upon the information received.

In general, all communication procedures and guidelines should be discussed with staff. Written procedures, as well as essential emergency contact information, including phone numbers, frequencies, and call signs should be posted in the office, each vehicle, and on a card for each staff member to carry.

It is important to test the systems regularly and have back up power supplies for radio, mobile/satellite phone charging.

Good practice:

- Staff never transmit sensitive information, such as the transfer of cash or travel plans, in plain language over the radio or phone networks.
- Communications equipment, including radios, cellular phones, and satellite phones, have the host nation government's approval and licensing prior to use.
- Where radios are used, multiple VHF and HF frequencies have been obtained for each office when possible.
- Use of other organisational radio networks – such as the United Nation's – has been coordinated.
- SMS, satellite phone calls or radio checks with remote offices and travellers in the area are routinely performed, as appropriate. A policy is in place in case a staff member or team fails to check in and cannot be contacted. All staff are familiar with this policy, and it is consistently implemented.
- Duress code words or phrases have been established for common emergency conditions such as kidnapping or intrusion. Their use has been discussed with staff.
- Radios and emergency phones are monitored 24 hours a day, as appropriate.

Information security

Regardless of how we view ourselves, international aid organisations are often no longer regarded as neutral, independent entities. They intervene, hold accountable, advocate and often subsume activities normally associated with governments (such as health care, water, sanitation and emergency relief), and in many occasions undertake these activities while funded by 'Western' governments with their own political agendas. This makes everything humanitarian NGOs do seem suspicious in many people's eyes.

See EISF briefing paper 'The future of humanitarian security in fragile contexts: an analysis of transformational factors affecting humanitarian action in the coming decade'

Governments usually have the means to monitor organisations' phone calls, internet activity, Facebook, Twitter and RSS feeds as well as hack your computer hard drives. Criminal organisations will also perceive NGOs as wealthy, given the vehicles, laptops, satellite phones they often use, as well as publicly announced donor funding levels. All of this makes aid agencies vulnerable to information security risks. Be aware that anything you write in an email can be read by criminals or government agents.

See EISF briefing paper 'Communications technology and humanitarian delivery: challenges and opportunities for security risk management'

Consider what to put into any shared drive. Emergency response staff often bring their own computers and will copy everything into a shared drive when they leave, for continuity. This may include inappropriate photos, personal information and context analysis that may be deemed insulting by other actors or staff. It is important to keep in mind as well what information – both business and personal – is kept on mobile devices such as smart phones, as this might easily be lost or stolen.

Assess the impact the information might have if it falls into the wrong hands – harassment of staff, dissemination of inappropriate photos, access to emails or office VPN/server, and so on.

Good practice:

- Back up all files regularly and keep back up copies of all key documents and records (government agreements, legal documents, bank records, HR records) off site in case of fire, flooding, theft or other event that destroys the originals.
- Paper documents also allow information leaks if they are left in bins or on desks for cleaners and other staff or visitors to see/copy/remove. Use shredders for any files not being kept in safe storage.
- Maintain good security firewall systems in any server and minimise staff access to networks with non-organisation computers, tablets or phones to prevent spread of viruses.
- Remember that Skype is no more secure against hacking than any other communication method.
- Never appear to be gathering 'intelligence' or passing any military or security information to foreign governments (including donors or your headquarters). Similarly, encrypting information may send the wrong message. Particularly if your NGO claims to be open and accountable, you may be questioned about the need to encrypt documentation.
- Avoid desktop computers when possible. Although laptops are easier to steal they are more mobile if the office or project needs to be relocated.
- Consider verification processes for information received via WhatsApp and other social apps that make it easier to share information directly between staff. There should be also clear guidance on what should and should not be shared.
- Ensure you have a social media policy that makes it clear to staff what they can and cannot post on social media sites.

See EISF guide 'Managing the message: communication and media management in a security crisis'

For technical tools and guidelines, 'Front Line Defenders' and 'Tactical Technology Collective' have developed *Security in-a-Box*, a guide to digital security for activists and human rights defenders. The guide covers the basic principles, including advice on how to use social networking platforms and mobile phones more safely, and also offers step-by-step instructions on how to install and use the most essential digital security software and services.