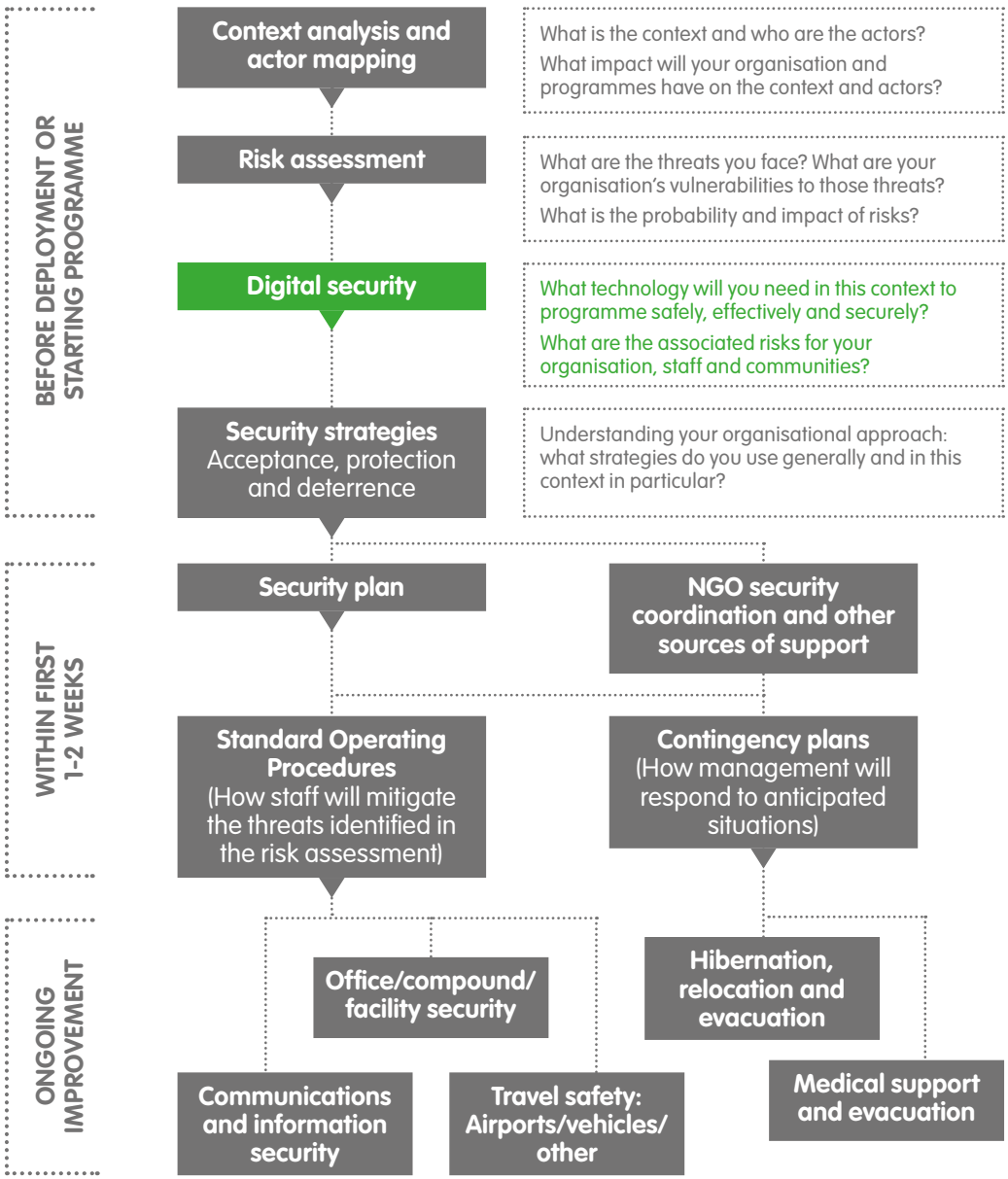
4 Digital Security



In the modern world, technology has become so entwined with our lives that we rarely pause to consider its implications. It becomes difficult to imagine life without our devices, and even more challenging to consider our work without associated software and apps, video calling, the cloud, emails, servers and the various accounts that help us to connect with our activities, colleagues and relatives. If technology is a powerful enabler, it is crucial to consider how this ever-present fact of life can put ourselves, our organisations, and our work, at risk.

This module provides basic advice for NGOs to integrate digital security within their overall security risk management processes.

Digital Security: The measures, strategies and processes that aim to mitigate risks related to organisations' and individuals' digital footprints and use of technologies.

Given the rapid pace at which technology evolves, some of the measures included in this module will need to be reviewed against up-to-date advice from reliable sources. There are many organisations that can provide digital security support and help you to build your policies. Among others, you can refer to the Frontline Defenders Digital Security & Privacy Handbook, the Digital First Aid Kit, the UK National Cyber Security Centre, Access Now, Security Without Borders and the Umbrella App.

Context analysis

To fulfil duty of care obligations and protect staff from physical and psychological harm, organisations must mitigate risks related to their digital presence and activities. When NGOs are starting a new project or entering a new region, both context analyses and risk assessments should therefore include digital security vulnerabilities.

When conducting a context analysis, consider exploring some of the following elements:

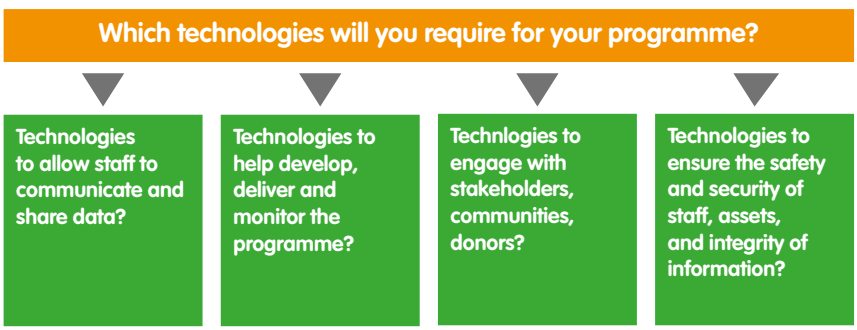
The legal context	**International/regional level** – For European-based organisations, data protection regulations such as the EU *General Data Protection Regulation* (GDPR) must be considered. They will affect how you collect, use and store data on individuals. It is also important to verify whether a Data Protection Impact Assessment (DPIA) is required for the data you are working with. **Country level** – Many nations are setting increased legal controls on technology. In several contexts, the use of equipment like radios and satellite phones are strictly controlled and may even be illegal. In other contexts, the use of encryption, as well as certain websites and social media, is prohibited.

The political context	**Government monitoring** - In areas where NGO support for the civil population is needed, the host government may be not only suspicious, but actively engaged in overt and covert monitoring of NGOs' activities, reports and communications. As well as this, home and donor governments increasingly require access to, and oversight of, the data handled by NGOs. Such involvement may carry serious implications for your programmes. While NGOs must adhere to the principle of transparency, we often possess information (on staff, beneficiaries and programmes) that is confidential in nature. **Network shutdowns** – Several governments have extensive control over communication networks and, in times of civil unrest, may declare internet shutdowns. Given NGOs' increasing dependence on technologies to operate, it is essential to consider this possibility and develop adequate plans to sustain communication channels.
The cyber crime context	This is often the most challenging area for NGOs. Not only do organisations need to assess locally-specific cyber risks, but they also need to be aware of the global cyber crime environment. Attacks on computers or mobile phones can be launched remotely and must be considered during travel.

Technology Needs Assessment

Every type of programme attracts different risks. Emergency response programmes may be more sensitive to blackmail, fraud or safeguarding threats. Advocacy and human rights campaigns may be targeted by various groups, seeking to damage the organisation, or to collect personal information on beneficiaries and staff. Development projects are also vulnerable to the diversion of resources and corruption. Even internally, NGOs use a range of technologies for their various operations, from communications to data gathering to implementation monitoring.

In order to accurately assess the threats that you may face and develop risk mitigation strategies, the first step is to identify what technology will be used. For this, you need to thoroughly understand your programme and consider the digital actions of the different stakeholders involved, such as staff, communities, donors and host governments.



Many NGOs are reluctant to explore new technologies due to the initial efforts required to train their staff and adapt their processes. However, when wisely incorporated into our activities, innovation can make programming both safer and more effective in the long term.

Technologies regularly used by NGO staff		
Equipment	**Communication devices**	**Software and apps**
Laptops/desktops/tablets External storage devices GPS/navigation systems Batteries/power-banks Vehicle tracking systems Scanners/printers Wireless devices	Smartphones/mobile phones Landline phones Satellite phones Radios/radio repeaters	Cloud-based file sharing Shared data servers WhatsApp and other messaging apps Skype and other video calling software Email Social media

Digital Risk Assessment

Understanding the digital risks that your staff, organisation and programmes face is a complex and difficult task – especially considering that cyber threats continually evolve. Many security advisers delegate this function to their organisation's Information Technology (IT) department, or to a trained member of staff. However, many digital incidents are not due to technical flaws, but rather due to 'digital misconduct' among staff. Improving an organisation's digital security, therefore, requires developing standard operating procedures (SOPs) and effective policies to guide staff in their use of technology.

Every staff member has a critical role to play in digital security!

Typical Digital Threats

Nowadays there are a wide variety of digital threats, which can affect both the organisation and its staff:

Organisation
• Hacking of files • Reputational damage, defamation • Communications monitoring or spying • Damage caused by viruses • Theft of devices • Fraud/financial theft • Misinformation/fake news • Theft of data pertaining to staff or beneficiaries

Staff
• Scamming, blackmailing • Movement tracking, targeting • Technology-induced stress • Fraud/financial theft • Misinformation/fake news • Theft of personal data • Identity theft

Online threats usually come in one of two forms:

- **Direct Attacks:** Attacks aimed at an individual or organisation's system for a specific purpose.

  Examples include: brute force (computer programmes attempting to break into a target computer by guessing possible combinations of a target's password), key loggers (virus softwares that identify passwords), proximity (direct surveillance).

- **Indirect Attacks:** Attacks of broad spectrum that often take the form of scams or phishing attempts, which may not be directly aimed at your NGO/staff.

  Examples include: phishing (fraudulent emails disguised as those from a trustworthy entity, which ask the recipient to perform certain actions such as clicking links or opening attachments).

Direct and indirect attacks can also be seen in social media environments, targeting either individuals' or organisations' accounts.

Don't forget to consider staff's diverse profiles when assessing threats. It is an organisation's responsibility to inform staff of the risks associated with the use of certain apps and technologies.

Particularly in countries where LGBTQ+ rights are not respected, staff can face serious threats from the use of specific dating apps (for example, being 'outed' online, blackmailing and physical assaults).

▶ *For further information, see EISF paper 'Managing the Security of Aid Workers with Diverse Profiles'.*

Digital Security Strategies

With your digital risk assessment complete, you should develop clear strategies to mitigate the identified risks. In recent years, staff misconduct and abuse scandals, combined with a rise in suspicion and political accusations, have placed NGOs in difficult positions and caused damage to their reputations. In addition,technological progress and the rise of social media has created a space where misconceptions and rumours can spread quickly, making NGOs ever-more vulnerable to reputational threats.

Given the importance of public perceptions and community acceptance for NGOs' access to populations in need, developing a clear digital security strategy is key for an operation's success. This document should fit within the general security policy and align with the organisation's approach to duty of care and security risk management.

The digital security strategy should cover three basic components:

Organisational Security	Staff Security	Community Security
• Internal network security (how will you establish a secure intranet, control access and protect data?) • If your NGO already has an internal network system in place, what confidential or sensitive information will this platform be collecting? • Acceptance/ reputational risk (how will you monitor and respond to negative accusations online?)	• How will you protect staff data (payroll and HR records, contact information, data stored on work devices)? • How will you maintain communications - especially in emergencies? • How will you support staff targeted by digital attacks? Do these measures protect staff with a diversity of profiles?	• How will you manage programme information to comply with 'do no harm' and safeguarding imperatives? • How will you comply with data protection regulations such as GDPR? • Can your existing feedback mechanisms and complaint response systems address online/social media abuse?

The digital security of staff, the organisation and the community is overlapping. Because a breach in one area will have repercussions for the others, it is important to consider their interdependence to devise a consistent and comprehensive approach to digital security.

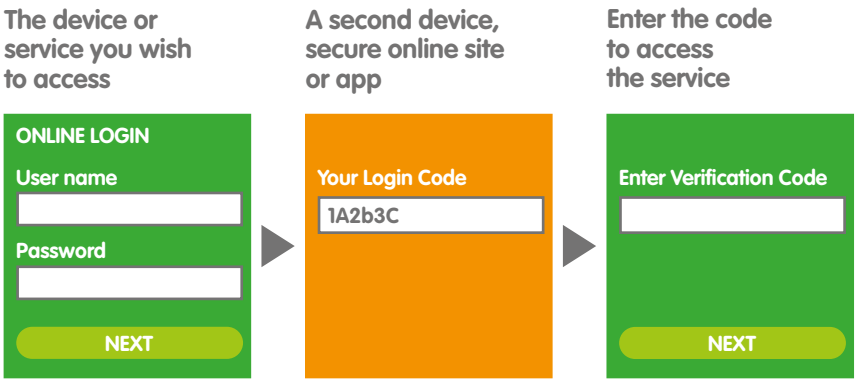
An inclusive strategy should take into account the specific risks faced by local staff and partners. In many instances, they are exposed to greater, and longer-term, repercussions from local governments and communities.

▶ *See GISF research paper 'Partnerships and Security Risk Management: From the local partner's perspective'*

Digital security policies should provide clear guidance on what is or is not allowed within the digital environment. They should cover the following points:

1. **Internal platform and devices:** Staff access and exit procedures, including the deletion of personal data, password protection mechanisms, anti-virus software/firewalls, protocols for data back-ups, software update regulations.

One mitigation measure is adding two-factor identification to all of your devices and key online services. This a valuable added security measure to prevent unauthorised access to your systems and devices.



2. **Information security:** Confidentiality policy and classification system - e.g. confidential, restricted, internal or suitable for public use, legally-compliant information sharing regulations.

Information security documents often refer to the three AIC principles:
1 availability (guarantee of access to information),
2. integrity (assurance that information is reliable) and
3. confidentiality (control of access to information).

See Module 9 - Communications and Information Security

3. **Communications:** Encryption regulations, audio-communications protocols, use of apps for work-related communications, log retention procedures.

Advise all staff to be cautious when following links in emails. Never open attachments in suspicious messages and beware of obscure file types such as .exe, .ink, .jar, .dmg, .wsf and .scr. Watch out for misspelled names and addresses – instead of 'a.person@your-ngo.org', a fraudulent address may read 'a.person@your-ngo.net'.

4. **Travel and network access:** Guidelines on the use of Virtual Private Networks (VPNs) or public or insecure networks, guidance and regulations on device protection).

Travel and network access policies are especially important for areas where governments and officials are suspicious of NGO activities, as there may be a heightened risk of monitoring and/or data theft.

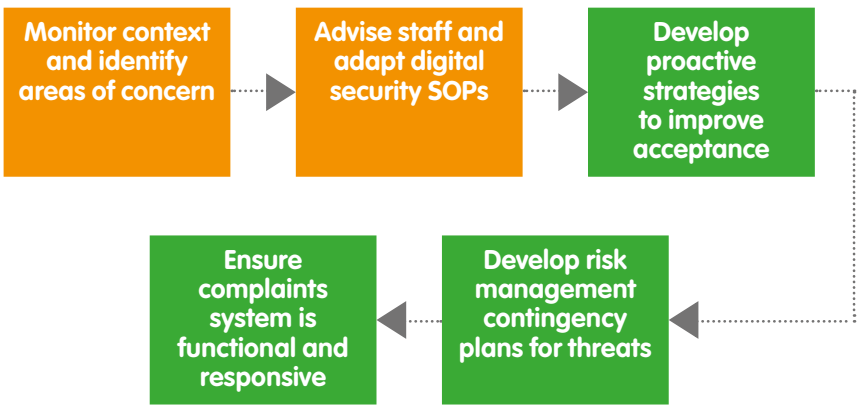
While wiping information from laptops, phones and other devices before travel may seem like a good security measure, this level of precaution can actually risk raising suspicion. When travelling, it is therefore preferable to keep only necessary, non-confidential information and avoid having devices too 'clean'. Consider using secure deletion tools such as CCleaner and Eraser. Doing regular back-ups of important files also prevents having your files ransomed.

5. **Social media:** Guidelines on posting sensitive information which align with the code of conduct, rules on the delay required when posting locations of travel (including geotagging), systems for reporting abuse and attacks against staff or the organisation).

Incorporating Digital Risk Management into Security Plans

Building on their existing security risk management policy, an office or programme team can develop a digital security plan that suits their current context and operational needs. Digital security challenges should feature as a component of the overall security plan to advise staff on the necessary risk mitigation procedures.

Constant monitoring of the local context and digital security environment is critical to the success of your programmes and the safety of your staff.



Training staff on digital security measures and regularly updating them on new and emerging threats is key. As technology-based risks evolve, we must ensure that staff are aware of the various threats that exist (for instance, malwares that can record audio, activate webcams, take screenshots and alter files) and that they adopt sound behaviours to mitigate associated risks.

Training should be adapted to the digital culture and competency of its public. In many regions, downloading pirated or copied softwares to work devices is common practice. Staff's social media habits and preferred communication apps (Whatsapp, Telegram, etc.) will also generate different risks – both to themselves and to the organisation.

HTTP versus HTTPS

All websites are identified by a Hyper Text Transfer Protocol (HTTP) leader in an online address. Websites that are verified as secure feature an HTTPS leader in the address line. Many modern browsers will provide a warning if you try to connect to a non-secure HTTP web address, or will block access entirely. Staff should be strongly advised against visiting insecure websites.

Below are examples of digital security measures that can be included in **Standing Operating Procedures** (SOPs). Note that these SOPs will need to be adapted to the relevant context analysis and risk assessment, as well as the wider programme and organisation.

Staff Network Access	• Staff can access the server only once they have completed a full HR induction. • Login must be completed only through the office server or the organisation's virtual private network (VPN). • Passwords should contain a combination of upper and lower case letters, numbers and special characters, and avoid using words that can be found in the dictionary. For example, *M*d0gH@zF!ea5* (my dog has fleas). • Do not record nor share your passwords and don't allow websites or browsers to store them. Instead use [insert organisation's preferred password management tool].
Data and information security	• All data contained on staff devices and server drives are considered confidential, including beneficiary data. • The release of any data outside of the organisation, including with specific donors and media must be approved by [insert relevant person]. • Conform to the confidentiality policy and use encryption for highly confidential communications for example, [insert organisation's preferred app] for mobile messaging.

Software and passwords	• All software and apps installed on devices provided by the organisation must be approved by [insert relevant person]. • Staff must install software updates immediately when notified. • Staff must not use the same password for multiple accounts, whether personal or work-related. • Staff must report all suspicious emails to [insert relevant person] and must never download attachments unless the sender is confirmed. • All devices must have privacy screens that auto-lock after a maximum of 3 minutes of non-use.
Staff travel	• Staff are responsible for ensuring that they have effective communications systems when travelling outside of main urban areas, and can recall their emergency numbers from memory. • When travelling to [insert relevant risk rating] areas, staff are advised to back up all personal and work files prior to travel. • Staff must not operate any devices while driving a vehicle.
Social Media	• Staff should not post any information online that is related to their work or travel plans, including via private social media accounts. • Stories or images gathered on the trip may be sent to [insert relevant person] for review and possible use by the organisation. • Staff must conform to the code of conduct in their personal social media activity at all times. • Staff should record abuses and report any online bullying or negative stories related to the organisation or its programmes to [insert relevant person].