# Security Risk Management Toolkit: Digital Security

READY to go Mobile Guide

Learn how to integrate digital security within your organization's security risk management processes.

## Digital Security

## Note to Learners

The information in this guide is for educational purposes only; it is not intended to be a substitute for professional or specialist security advice. Any reliance you place on such information is therefore at your own risk and the Global Interagency Security Forum (GISF) will have no responsibility or liability under any circumstances.

# Digital Security Risk Management

Technology is a powerful enabler that helps us to conduct important activities and connects us with colleagues and others across the world. Relief and development organizations increasingly depend on technology and devices to carry out programming and operations, especially from remote locations.

While technology and innovation can help us work more effectively, it is important to consider our digital footprint and how using different technologies can put employees, organizations, and communities at risk.

Digital security risk management consists of measures, strategies, and processes used to mitigate risks and to secure the identity, data, assets, and devices of individuals and organizations.

## Context Analysis

When organizations start a new project or begin working in a new region, their context analysis and security risk assessment should also include digital security vulnerabilities. Consider these elements when conducting a context analysis.

### Legal Context at International/Regional Level

Understand international and regional legal regulations on technology:

- Verify if a Data Protection Impact Assessment (DPIA) is required for the data you are managing.
- For European-based organizations, refer to data protection regulations such as the EU General Data Protection Regulation (GDPR) on how to collect, use, and store data on individuals.

### Legal Context at Country Level

Know the legal controls on technology in the countries in which your organization is working. In some contexts, the following may be strictly controlled, prohibited, or even illegal:

- Using equipment such as radios and satellite phones
- Using encryption
- Accessing specific websites and social media

### Government Monitoring

In areas where humanitarian support for the civil population is needed, be aware that host and/or donor governments may:

- Be suspicious of humanitarian organizations and staff
- Actively engage in overt and covert monitoring of organizations' activities, reports, and communications
- Require access to sensitive data and confidential information about staff, communities, and programs which could have serious implications for an organization, its programs as well as affected populations in the area

### Network Shutdowns

Be aware that some governments may:

- Have extensive control over communication networks
- Declare internet shutdowns during times of civil unrest

Determine if these circumstances apply to your working environment and develop adequate plans to maintain your organization's communication channels.

### Cybercrime Context

Take actions to prevent cybercrime against your organization by:

- Being aware of the global cybercrime environment
- Assessing local cyber risks
- Mitigating risks of attacks on computers/mobile devices that can be launched remotely and/or during travel

# Digital Risk Assessment

## Identifying Digital Risks

**Every staff member has a critical role in digital security risk management.**

Identifying digital risks that your organization, its staff, and programs may face is a complex and difficult task, especially considering that cyber threats continually evolve. Many digital incidents are not caused by technical flaws but are due to 'digital misconduct' of staff.

Improving your organization's digital security requires conducting comprehensive digital security risk assessments and developing standard operating procedures (SOPs) and policies to guide staff on how to safely use technology.

# Assessing Technology Needs

Different types of programs and projects attract different types of risks. Emergency response programs may be more susceptible to risks of blackmail, fraud, or safeguarding threats. Advocacy and human rights campaigns may be targeted by different groups seeking to damage the organization or to collect personal information on communities and staff. Development projects may be vulnerable to the diversion of resources and corruption.

Your organization may use a range of technologies to conduct operations for different purposes, including communications, data collection, implementation, and monitoring. As part of the digital security risk assessment, it is critical for your organization to identify the different technologies they are using and consider how different stakeholders may use them (staff, communities, donors, host governments) in order to accurately assess potential digital threats and develop risk mitigation strategies.

Which technologies does your organization require for its programs?

- Technologies to allow staff to communicate and share data
- Technologies to help develop, deliver, and monitor programs
- Technologies to ensure the safety and security of staff, assets, and the integrity of information
- Technologies to engage with stakeholders, communities, and donors

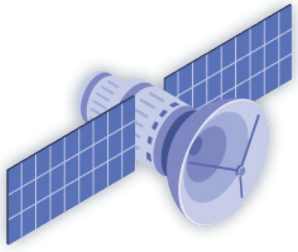
# Using Equipment and Devices

During the digital risk assessment process, the assessment team should consider the specific types of equipment, devices, and software that staff need for work, and identify potential risks of using them.

**Equipment**

- Laptops/desktops/tablets
- External storage devices
- GPS/navigation systems
- Batteries/power-banks
- Vehicle tracking systems
- Scanners/printers
- Wireless devices

**Communication Devices**



- Smartphones/mobile phones
- Landline phones
- Satellite phones
- Radios/radio repeaters

### Software and Apps

- Cloud-based file sharing
- Shared data servers
- Messaging apps (WhatsApp, Telegram)
- Video calling and conferencing software (Skype, Zoom)
- Email
- Social media

## Identifying Digital Threats

There is a wide range of digital threats that can affect your organization and its staff. Your organization is responsible for informing staff of the risks associated with using certain apps and technologies. To adequately protect all employees, your organization needs to consider the diverse profiles of staff when identifying potential digital threats.

### Digital Threats for Staff

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


**Important:** In countries where LGBTIQA+ rights are not respected, staff who use certain dating apps may be vulnerable to threats such as blackmail, physical assault, or being 'outed' online.

### Digital Threats for Organizations

- Hacking 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

# Forms of Online Attacks

Organizations are increasingly exposed to online threats. Online threats are usually categorized in two forms: **direct attacks** and **indirect attacks**.


### Direct Attacks

Direct attacks are aimed at an individual or organization's system for a specific purpose.

Examples:

- **Brute force** = computer programs attempting to break into a target computer by guessing possible password combinations
- **Key loggers** = virus software that identifies passwords
- **Proximity** = direct surveillance
- **Social media attacks** = targeting accounts of individuals or organizations


### Indirect Attacks

Indirect attacks often take the form of scams or phishing attempts which may not be directly aimed at an organization or its staff.

Examples:

- **Phishing** = fraudulent emails disguised as being sent by a trustworthy entity which ask recipients to perform certain actions, such as clicking links or opening attachments

# Digital Security Strategies

## Developing a Digital Security Risk Management Strategy

Once the digital risk assessment is complete, your organization should develop a solid Digital Security Strategy that mitigates the identified risks. Address these critical security considerations when developing your organization's strategy.


Ensure the strategy fits within the organization's general security policy.

Align the digital security strategy with the organization's approach to duty of care and security risk management.

Consider how digital security mutually affects staff, the organization, and the community. Analyze how a security breach in one area could impact other areas.

Understand how the diverse profiles of staff can make them vulnerable to different digital security risks. For example, national staff and partners may be exposed to greater, long-term repercussions from local governments and communities if the confidentiality of their personal information is breached.

Consider how your organization will address online threats that may affect its reputation, credibility, and acceptance among affected populations. This includes being aware of how social media can create a space where misconceptions and rumours spread quickly, making NGOs more vulnerable to reputational threats.

# Elements of a Digital Security Risk Management Strategy

Your organization's digital security strategy should cover three basic components: organizational, staff, and community security.

### Organizational Security

Think about the security of your organization:

- How will you establish a secure internal network system (intranet, control access, data protection)?
- What confidential or sensitive information will the internal network system be collecting?
- How will you monitor and respond to negative accusations online that threaten your organization's acceptance and reputation?

### Staff Security

Think about the security of staff:

- How will you protect staff targeted by digital attacks?
- Do security measures safeguard all staff with different profiles?
- 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?

### Community Security

Think about the security of the different communities with which you work:

- How will you manage program information to comply with 'Do No Harm' and safeguarding policies?
- How will you comply with data protection regulations such as General Data Protection Regulation (GDPR)?
- Are your existing feedback mechanisms and complaint response systems addressing online and social media abuse?

# Defining Digital Security Risk Management Policies

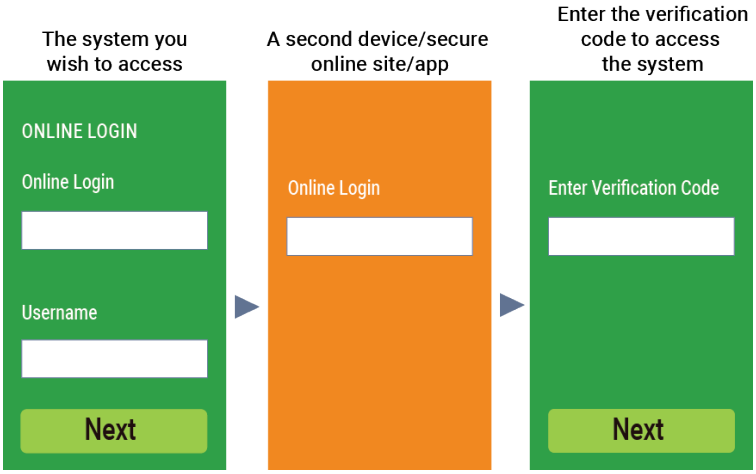
Digital security policies should provide clear guidance on what is allowed or what is not allowed within the digital environment. Consider these elements when developing your organization's digital security risk management policies.

### Internal Systems and Devices

Staff access and exit procedures to internal systems and devices, including:

- Deletion of personal data
- Password protection mechanisms
- Anti-virus software and firewalls
- Protocols for data backups
- Software update regulation

Example: Adding two-factor authentication to all organizational systems and devices is an effective security measure to prevent unauthorized access.




### Information Security

Establish a confidentiality policy and classification system for information security. This should include guidelines for confidential, restricted, internal, or public materials, and legally compliant information sharing regulations.

Information security documents often refer to the three **AIC** principles:

- **Availability** (guarantee of access to information)
- **Integrity** (assurance that information is reliable)
- **Confidentiality** (control of access to information)

**Communications**

Establish digital security policies for communications including:

- Encryption regulations
- Audio-communications protocols
- Guidance on the use of apps for work-related communications
- Log retention procedures
- Advice for staff on suspicious emails

Examples:

- Never open attachments in suspicious messages
- Avoid obscure file types (.exe, .ink, .jar, .dmg, .wsf and .scr)
- Watch out for misspelled names and addresses (a fraudulent address may display 'a.person@your-ngo.net' instead of 'a.person@your-ngo.org')

**Travel and Network Access**

Travel and network access policies are especially important for areas where there is a heightened risk of monitoring and/or data theft by the government/officials who may be suspicious of your organization's activities. Policies should include:

- Guidelines for using Virtual Private Networks (VPNs) and public or insecure networks
- Guidance and regulations on device protection (Example: Conduct regular backups of important files to prevent them from being stolen or ransomed.)
- Guidelines for travel (Example: Wiping information from devices before travel may seem like a good security measure, however, this level of precaution can actually raise suspicion. When traveling, keep only necessary, non-confidential information and avoid keeping devices too 'clean'.)

**Social Media**

Establish social media policies that include:

- Guidelines on posting sensitive information (which are aligned with your organization's code of conduct)
- Systems for reporting abuse and attacks against staff or the organization

**Digital Security Training**

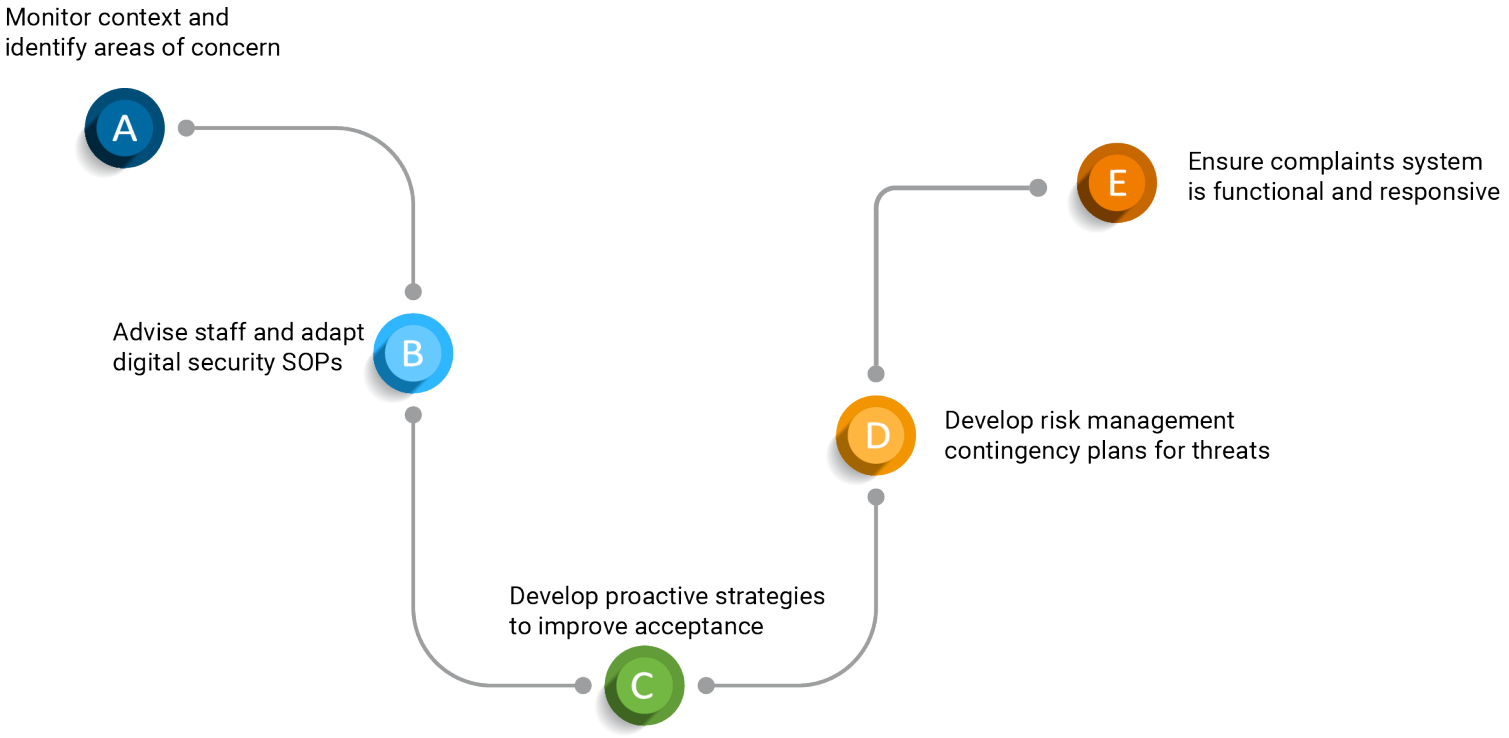
As technology-based risks evolve, continuously inform and train staff on digital security measures and regularly update them on new and emerging threats. Make sure to adapt the training to the digital culture and competency of your staff. Ensure that all staff are aware of the different risks that exist and how these risks can impact them, their colleagues, and the organization. They should understand how to mitigate potential risks, which may include:

- Technology-based threats (malwares that can record audio, activate webcams, take screenshots, or alter files)
- Risks from using social media and communication apps (WhatsApp)
- Risks associated with visiting insecure sites (staff should only connect to secure websites that have an 'HTTPS' web address)
- Risks associated with using pirated or copied software

## Digital Security Plan

# Incorporating Digital Risk Management into Security Plans

Constant monitoring of the local context and digital security environment is critical to the success of your organization's programs and the safety of staff. Building on existing security risk management policies can help you develop a **Digital Security Plan** that suits the current context and operational needs of a specific program or office. The Digital Security Plan should include digital security challenges and advise staff on risk mitigation procedures.



# Integrating Digital Security Measures into SOPs

Organizations should include digital security measures in their **Standing Operating Procedures (SOPs)**. It is important to adapt SOPs according to your organization's context analysis, risk assessment, and wider programming. Consider how some of these digital security measures can be incorporated into your organization's Standing Operating Procedures.

**Staff Network Access and Passwords**

**STAFF MUST:**

- Complete a full employee induction process before gaining access to the server.
- Log in only through the office server or the organization's virtual private network (VPN).
- Use passwords that contain a combination of upper and lower case letters, numbers and special characters, and avoid using words that can be found in a dictionary. Good Password Example: M*d0gH@zF!ea5 (my dog has fleas)
- Use the organization's preferred password management tool (if available).

**STAFF MUST NOT:**

- Record or share passwords.
- Use the same password for multiple accounts, whether personal or work-related.
- Allow websites/browsers to store passwords.

**Data and Information Security**

**ORGANIZATIONS SHOULD:**

- Consider all data contained on staff devices and server drives as confidential, including beneficiary data.
- Designate a staff member who approves the release of any data outside of the organization, including donors and the media.
- Ensure that data collection and information security processes comply with the organization's confidentiality policy.
- Encourage the use of encryption for highly confidential communications.
- Select a preferred app to use for mobile messaging at work.

**Software**

**STAFF MUST:**

- Seek approval from the designated focal point to install software and apps on devices provided by the organization.
- Install software updates immediately when notified.
- Use privacy screens on work devices that auto-lock after three minutes or less of non-use.
- Report all suspicious emails to the designated focal point.

**STAFF MUST NOT:**

- Download attachments unless the sender is confirmed.

**Staff Travel**

**STAFF MUST:**

- Ensure that they have effective communications systems when traveling outside of main urban areas.
- Memorize emergency numbers.
- Back up all personal and work files BEFORE traveling to high-risk areas.
- Keep only necessary, non-confidential information on their devices (and avoid keeping devices too 'clean') when traveling to high-risk areas.

**STAFF MUST NOT:**

- Operate any devices while driving a vehicle.