

gisf



## Section A: Policy and Planning

# Module 2: Information management



# Section A: Policy and Planning

## Module 2: Information management

### Introduction to the series

The pandemic continues to impact not only the security risks that NGOs may face but also the way risk treatment measures are developed, implemented and communicated to staff.

As we get used to new ways of working with COVID-19, and the focus is, rightly, on the pandemic and its impacts, we must ensure that we do not lose sight of ongoing and emerging security situations and issues.

### Introduction to the module

Good information management practice is key to informing decision-making, assisting organisations in fulfilling their duty of care to staff and ensuring that staff feel safe and cared for by their organisation.

The volume of information required to inform decision-making in humanitarian and development organisations rose exponentially as COVID-19 became a pandemic. One of the biggest challenges has been the quantity and speed of available information, disinformation and misinformation.

Some examples of external information that have been changing daily include how and where the virus is spreading, government and local authority containment measures, travel restrictions, approaches to quarantine and the overall security context.

### Acknowledgements

This module was written by Heather Hughes and Lisa Reilly of GISF, with additional input from Christina Wille of Insecurity Insight and James Blake, an independent journalist and author of the GISF Blog piece, [Disinformation of Security Risk Management for NGOs](#).

### Suggested citation

GISF. (2020) *Keeping up with COVID-19: essential guidance for security risk managers, Module A.2. Information Management*. Global Interagency Security Forum (GISF). First Edition, August 2020.

---

### Disclaimer

GISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'GISF' in this disclaimer shall mean the member agencies, observers and secretariat of GISF.

The content of this document is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this document.

While GISF endeavours to ensure that the information in this document is correct, GISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, GISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. GISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

© 2020 Global Interagency Security Forum

## Why is information management important during the COVID-19 pandemic?

### Duty of care

Organisations must be able to demonstrate that they have identified and considered all foreseeable risks related to a particular location or activity. COVID-19 is a foreseeable risk that must be assessed, mitigated, and managed, as per any other specific risk. Information management is necessary to be able to track and manage this process.

Organisations must ensure that staff continue to trust them to provide accurate information and to look after their welfare. This is particularly difficult with the amount of contradictory information on COVID-19 available to all staff (headquarters (HQ), country offices, partners) from multiple mainstream media and social media outlets, rather than the specialist media coverage that humanitarian crises receive.

### Further information

.....

*Bickley, S. (2017) Security Risk Management: a basic guide for smaller NGOs. European Interagency Security Forum (EISF). Page 8: Your Duty of Care.*

.....

### Risk attitude and threshold, and the ability to deliver programmes and objectives

Organisations have a wide range of mandates, values, and cultures, and an equally wide range of ways of working and delivering programmes and objectives. Those working in high risk environments may have already conducted an exercise to determine the level of risk they are willing to accept and manage for the type of programmes they are delivering.

In light of COVID-19, this will need to be reviewed, considering new and changing threats relating directly to the pandemic, the impact of the containment measures and the ability of HQ - who may have been directly impacted - to provide support and manage risks to staff and offices globally. The direct management support that HQs can provide needs to be considered in determining the revised risk threshold.

Good information management is necessary to help organisations make informed decisions about their risk threshold, the types of programmes they are willing to deliver and their ways of working.

### Further information

.....

*Bickley, S. (2017) Security Risk Management: a basic guide for smaller NGOs. European Interagency Security Forum (EISF). Page 9: Defining Risk Attitudes.*

.....

### Disinformation and misinformation at local and global levels

Misinformation and disinformation are often used interchangeably, but have different meanings; the former is false information given without malice and the latter is false information, given with the intention to deceive. In the current pandemic, when accurate information can save lives, false information can have seriously negative consequences. False information about COVID-19 has spread quickly and widely through social media, text messaging and mass media. The World Health Organisation (WHO) has referred to an ‘infodemic’ of incorrect information, and stated that it poses a risk to public health.

The high volume of false information makes it hard to distinguish what is helpful and useful information, and what measures and approaches are right to follow. It can also be dangerous, creating an atmosphere that has encouraged attacks - particularly on health workers - in some countries.

Misinformation and disinformation range from opinion to false accusations, hate speech, conspiracy theories and attempted hacks and scams.

Examples include:

- Conspiracy theories about the scale, origin, prevention methods and vaccine development related to the virus.
- False health information regarding bogus cures and treatments.
- Hackers and scammers posing as health authorities sending fraudulent email and text messages attempting to trick people into clicking on malicious links or opening attachments in order to steal money or sensitive information.

Keeping well informed about factually correct information, as well as about false information and common perceptions in different locations, is necessary in order to be able to support staff with accurate, useful, and effective information to mitigate and manage the risks of COVID-19.

Where deliberate disinformation is concerned, it is important to understand the motivation behind it, for example, local political gains, fuelling anti-western sentiment and/or global politics. It is also essential to understand how community perceptions of aid, your NGO and the international community may have changed since the outbreak of COVID-19, as this will have a direct impact on your acceptance strategy.

### Useful sources

.....

**GISF:** [Coronavirus \(COVID-19\)](#).  
*Useful resources, tools, and guidance.*

**Insecurity Insight:** [Aid Security and COVID-19](#).  
*Insecurity Insight is using open-source media monitoring and working with GISF and partner aid agencies who share their incidents, to help the aid sector gain a better overview of the developing situation.*

**WHO:** [Coronavirus disease \(COVID-19\) advice for the public: myth busters](#).

**WHO:** [Coronavirus disease \(COVID-19\) pandemic](#).  
*COVID-19 information including travel advice, country guidance, and training videos.*

**Johns Hopkins University:** [COVID-19 Dashboard](#).

**Internews:** [Internews program addresses global 'info-demic' on COVID-19](#).  
*Reporting and resources guidance for journalists in Southeast Asia.*

.....

### Attacks on aid workers

Since containment measures and lockdowns were introduced in many countries the numbers of reported aid agency security incidents fell sharply in some locations from mid-March (source Insecurity Insight, COVID-19 bulletin 5) due to most organisations limiting all staff movement. However, violence against frontline health workers

responding to COVID-19 rose dramatically after the WHO's pandemic declaration.

Reported incidents include violent responses to testing, quarantine measures and attacks against health workers arising out of fear that they could spread the infection.

GISF coordinated with Insecurity Insight, in the early days of the pandemic, to encourage organisations to share information regarding COVID-19 related security incidents. Regular updates have been produced to get a better understanding of the developing situation though tracking incidents and events.

It is anticipated that attacks will increase as the global economic impact of the pandemic is felt and distribution centres, storage facilities and perceived 'wealthy' locations may be the target for civil unrest and looting.

### Reputational risks

There may be serious reputational and consequent security risks to organisations, or possibly to the wider aid sector, if staff are perceived to have, or have in practice, spread the infection to communities or others. Information concerning infections in staff must be extremely well managed, both internally and externally, and health information about specific individuals must remain confidential.

### Containment measures and travel restrictions

Wide-ranging measures have been introduced by national governments, health authorities and other local authorities in many countries to curb the spread of the pandemic. Examples include total lockdowns - leaving home only for essential food shopping, medical reasons, or limited forms of exercise, restrictions on travel between certain locations, restrictions on entry to refugee camps and quarantine on arrival in airports. Understanding the measures that are in place in all locations of operation is necessary to continue to operate within local guidance and legislation, while protecting staff from potential pandemic risks as much as possible.

## Useful sources

ACAPS: [Government and local authority restrictions and containment measures by country.](#)

World Food Programme (WFP): [World Travel Restrictions.](#)  
*Realtime information database and situation response about the global travel restrictions put into place as a response to the spread of COVID-19.*

International Civil Aviation Organization (ICAO): [Global COVID-19 Airport Status.](#)  
*This app displays COVID-related information per State including information on airspaces/airports as available through the NOTAM service.*

United Nations (UN): [COVID-19 Coordinators.](#)

## Context-specific updates

The security situation is constantly changing in many locations due to the prevailing situation. COVID-19 is an additional factor that may be affecting contexts in different ways, as outlined above.

## Useful sources

ACAPS: [COVID-19 Field Updates.](#)  
*Focus on impact on essential health services, access and availability of regular goods and services, humanitarian operations, social cohesion and protection, and country reports.*

UN: [COVID-19 Coordinators.](#)

Business Risk Management companies are offering various COVID-related information services. If you have travel or medical insurance, or other such services, check with your provider if they are producing regular information bulletins.

## Good practice for security risk management: information management

### Information management is a two-way process

The organisation must assign responsibility for information management to specific individuals or roles. The key tasks are gathering, collating, and analysing information from external sources to provide effective and timely information to support management in decision-making and keep staff informed; listening to feedback from all staff about their concerns and the practicalities of their day-to-day work, and finally, ensuring that staff's voices are heard and acted on by decision makers.

### Continue to report incidents

Staff must be encouraged to continue to report security incidents in the usual way for the organisation; they should be reminded that the timely reporting of incidents can be critical for protecting staff and others in the community.

Consider sharing your organisational incident reports with other organisations locally, as well as with Insecurity Insight, who are undertaking analysis of trends for the benefit of the sector.

As well as recording incidents that directly impact your organisation, tracking changes in the wider threat environment is important. COVID-19 and consequent government containment measures may result in civil disobedience and other community-based actions, thereby possibly creating new threats in your areas of operation. Staff should be reminded of what needs to be reported, including wider contextual changes and direct security incidents.

## Further information

Bickley, S. (2017) *Security Risk Management: a basic guide for smaller NGOs.* European Interagency Security Forum (EISF). Section 8: Incident Monitoring.

[www.gisf.ngo](http://www.gisf.ngo). [Reporting COVID-19 related security incidents.](#)

[www.insecurityinsight.org](http://www.insecurityinsight.org). [Mobile guides and podcasts](#).

## Security plans and procedures

Most organisations should already have in place country security plans based on long-term risk assessments, as well as accompanying travel management procedures and others, such as evacuation or crisis management plans. All plans and procedures need to be reviewed in light of the pandemic to reflect the impact of COVID-19 in the specific location and significant changes to the organisation's approach, to the relevant programme, and to the organisation's ability to provide management support.

For example, has there been a shift from international to national staff or partner-management of projects? Do security plans reflect the specific risks that national staff and partners may face? In the event of an incident, are HQ staff able to provide the usual level of management support? Regular reviews will need to be undertaken as new information emerges, such as research on the differentiated impacts of COVID-19.

Particular consideration should be given to medical support and evacuation for COVID-19 and non-COVID-19 related cases as access to medical facilities and options for medical evacuation have been severely impacted.

Although the numbers of some types of security incidents fell sharply after mid-March, attacks on aid workers, unrelated to COVID-19, have continued. The number of critical incidents such as kidnapping and killing of aid workers in sub-Saharan Africa, has not really changed compared to long term trends. Organisations must remain vigilant and ensure that regular approaches to security risk management are being practiced.

## Security and safety briefings

As risk assessments and security and safety plans and procedures are reviewed and updated, all staff will need to be regularly updated and given the opportunity to give feedback.

## Internal communication

Because of the volume, speed and mixture of accurate information, misinformation and disinformation in circulation, organisations need to provide regular, correct information updates. Staff are likely to be informed by mass media, social media, and friends and family, so establishing the organisation as the key authority will help to build and maintain trust.

In addition to maximising the use of current information dissemination channels, the adoption of new methods and technology such as dashboards, video, and meeting platforms should also be considered.

### Internal communications: what your staff need to hear

- Provide staff with clear and simple information about what action they should be taking personally, and what actions and measures your organisation is planning and implementing, based on facts and reputable guidance.
- Misinformation and disinformation should be tackled openly and countered based on reputable sources.
- All communication needs to be consistent, concise, and considerate.
- Information, guidance, and instruction for staff must be consistent with local law and regulations, issued by health and other authorities in each country you work in.
- Staff must be informed as soon as possible about incidents and events in the countries they work in, which may have a bearing on their security and safety.
- Staff need to be regularly updated on reviews to security and safety plans and procedures, and given the opportunity to feedback concerns and questions.

## Inclusivity considerations for information management

Although COVID-19's reach may be global, its impact is far from consistent. The health risks of the virus are not equal. On top of the well-documented impact of COVID-19 on older people and those with pre-existing conditions, [data from the UK Office for National Statistics](#) show that, in the UK, black men and women are more than four times as likely to die from the virus compared to people of white ethnicity.

Developing an inclusive approach to security risk management based on effective, up-to-date information management and ensuring approaches are adapted to reflect best practices for operating within the pandemic are urgent responsibilities for organisations.

The 2018 GISF research paper 'Managing the Security of Aid Workers with Diverse Profiles' outlines how personal characteristics can impact the safety and security risks that individuals face. These include sex, gender, ethnicity, cognitive and physical abilities and sexual orientation.

Some risks are unique to certain individuals based on these characteristics. However, other risks exist for the majority of staff, but are more or less likely for some than others. The paper suggests that an aid worker's personal security is impacted by the interplay between:

- Where the aid worker is (context)
- Who they are (personal characteristics)
- And their role and organisation.

Given the different levels of risk relating to COVID-19, depending on aid workers' risk profiles (as described above), staff and partners must be kept informed of risks and the organisation's approach to risk treatment. Opportunities for feedback need to be outlined and encouraged to ensure that information is two-way. Key issues include:

- Providing sufficient information for informed consent during re-deployment and re-entry to the workplace.
- Sharing risk assessments and security plans with staff before returning to work, to allow them to raise concerns about particular risks, and provide time to put in place proactive measures to address risks for staff with particular vulnerabilities.

- Reminding all staff of the incident reporting mechanisms available to them, including any specific infection reporting mechanism.
- Providing clear guidelines outlining how the organisation will carry out contact tracing.

### Further information

.....








EISF. (2018) *Managing the Security of Aid Workers with Diverse Profiles*. European Interagency Security Forum (EISF).

Sweeney, A. (2020) *Adopting an inclusive approach to aid worker security risk management in the COVID-19 era*.

.....

## Conclusion

Information management is key for effective and safe implementation of programmes and is even more critical during the COVID-19 pandemic.

-  The sheer quantity of information, misinformation and disinformation available on COVID-19 creates special challenges for information monitoring, analysis and management.
-  COVID-19's dynamic and complex global situation and its potential impact on staff security and wellbeing must be understood and acted on appropriately at local, national and international levels.
-  Information management is two-way and organisations need to listen to their staff and take a compassionate approach to concerns.
-  Factually accurate information should be provided for all staff on a timely and regular basis in order to develop and maintain trust.
-  Regular monitoring of local information sources is essential to understand how perceptions and threats may be changing within the specific context.
-  Security plans and procedures should be regularly updated to reflect changes in the context.
-  Information about infections affecting staff must be well managed internally and externally.