

## 5.3 Security communication within the organisation

In the complex environments where aid organisations operate, effective communication of security information is not just a procedural necessity: it is also a critical component of protecting staff and ensuring the continuity of humanitarian work. The better informed a staff member is, the more likely they are to understand and comply with the security risk management processes put in place by their organisation. Moreover, well-disseminated and high-quality information can help alleviate the anxiety and uncertainty that often accompany work in volatile or high-risk environments.

### 5.3.1 Person-centred communication

A key principle in the dissemination of security information is to adopt an approach that is both person-centred and audience-specific. Unlike traditional models that may focus on the organisation's needs, this method prioritises the specific concerns, vulnerabilities and requirements of the individuals at risk, while also tailoring the communication method to the target audience. Whether the information is shared individually through briefings or collectively via intranet pages or SMS alerts, content and delivery should be adapted to suit the recipients. This approach not only ensures compliance with security protocols, but also actively engages staff by making the information relevant to their immediate circumstances and personal security.

For instance, when briefing an individual staff member about risks in a high-risk environment, it is crucial to consider factors such as their background, experience and role within the organisation. A generic briefing might not sufficiently address the particular risks faced by a female staff member travelling alone in a conservative region, or a staff member with health vulnerabilities. When addressing larger groups via Intranet or SMS alerts, the information should be clear, accessible and tailored to the common concerns of the group, while still allowing for individual considerations where necessary.

Security staff need to be creative about how they share information.<sup>84</sup> Language, formats and channels all need to be considered. Visual aids like infographics,

84 Storytelling, for example, can be an effective way to engage staff in security training courses. For more, see Persaud, C. (2022) *Storytelling for learning: using engaging, ethical stories for effective security training*. GISF (<https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/>).

maps and flowcharts can help make complex information easier to digest, and plain language, clear instructions and avoidance of technical jargon can significantly enhance the effectiveness of communication.

Ultimately, the goal of security communication is not merely to inform but to empower. Staff need to be able to understand not only what they need to do, but also why it is important as this increases the likelihood of compliance and helps to build a positive security culture. By providing staff with the targeted information they need to understand and navigate the risks they face, organisations can help them to work safely and effectively, even in the most challenging circumstances.

- ▶ See Chapter 1.2 for more on a person-centred approach to security.
- ▶ See Chapter 1.1 for more building a positive security culture.

### 5.3.2 Modes of information dissemination

The effectiveness of security information dissemination largely depends on the channels and methods used.

- **Organisational webpages for staff (intranet).** Intranets are a valuable tool for disseminating security information. Organisations can use the intranet to post regular updates on the security situation, changes in risk levels and updates to security protocols. There may also be specific pages providing guidance to staff with particular identity profiles. However, intranet relies on functioning networks, which might not always be available for all staff.
- **Email.** Email remains a key channel for disseminating information within aid organisations. To be effective, emails need to be clear, concise and structured, with important information prominently displayed. Urgency indicators, such as priority flags and clear subject lines, help ensure that critical messages are not overlooked. Regular updates are crucial in ongoing situations, while translation into staff members' primary languages avoids misunderstandings (sometimes providing links to AI translators can be sufficient). It may be beneficial in some circumstances to request that staff confirm receipt and understanding of emails, particularly for critical communications.
- **Mobile phone alerts (such as SMS or apps like Signal and WhatsApp).** Alerts sent to mobile phones provide a direct and immediate means of communication, ensuring that critical information is delivered to staff even when they are travelling or working remotely. These alerts are particularly useful in scenarios where rapid dissemination of information is required, such

as during a sudden escalation in violence or an unexpected disaster. However, it is crucial to balance the frequency of alerts to avoid overwhelming staff with excessive messages, which could lead to important alerts being overlooked.

- **Briefings.** Travel-related briefings are an essential part of security information dissemination, especially for staff members who are about to enter a volatile or unfamiliar environment. As situations can change rapidly, it is important to provide updated security briefings regularly to affected staff. Briefings should never be a one-off event.
- See Chapter 7.1 for more on guidance on briefings and travel-related risks and mitigation measures.

- **Situation reports (sitreps).** Sitreps are a crucial tool for keeping staff informed of the prevailing security situation. These reports should be able to be produced quickly, be concise and focus on providing up-to-date situational information that is easily digestible. A well-crafted sitrep not only outlines the current security environment, but also highlights potential implications for the organisation's operations and any changes that may be required to procedures.

Sitreps have a fairly familiar format, but should still be tailored for their audience and purpose. Sitreps for project staff focus on actionable advice and immediate risks, while those written for senior management might include a broader analysis of trends and potential future scenarios.

- **Reports.** In addition to more immediate updates provided by sitreps, organisations may produce analytical reports that offer a deeper examination of security trends and risks. These reports can be triggered by significant situational or contextual shifts and are designed to inform strategic decision-making within the organisation. Analytical reports can also be time-bound, such as monthly or quarterly assessments, and may include a range of media and other resources.

While these reports are less likely to result in immediate procedural changes, they play a critical role in shaping the organisation's long-term security strategy. For example, a report might highlight emerging threats in a particular region that could affect the organisation's future operations, leading to a review of risk assessments and contingency plans. Given the strategic nature of these reports, it is essential that they are written with the intended audience in mind. Senior management, for instance, may require a more detailed analysis of the potential impact on operations, while operational staff might benefit from summaries that focus on the practical implications for their day-to-day activities.

- ▶ See Chapter 4.4 for more on analysis of security incident trends.
- ▶ See Chapter 3.4 for more on security monitoring mechanisms.

### 5.3.3 Managing information overload

One of the significant challenges in security information dissemination is the risk of information overload, particularly in volatile environments where events can unfold rapidly. In such situations, the sheer volume of information can overwhelm staff, making it difficult for them to absorb and act on the most critical updates. A triage system prioritises information based on its urgency and relevance.

The triage system should be guided by a series of key questions and considerations:

- **Operational importance.** Will the safety and security of staff be compromised if this information is not passed on immediately? If yes, share immediately. If not, consider the point(s) below.
- **Situational update.** Does the information indicate a potential effect on security, possibly indicating the need for heightened precautions? If yes, inform relevant staff in a timely manner. If not, consider the point below.
- **Context shift.** Does the information indicate a trend or other longer-term implications for the programme environment? If yes, consider when and how best to use the information to inform strategic decision-making.

Each organisation will need to consider the best way to transmit security information for each level, and ensure staff are trained on how and when to share this information, and with whom.

For information that has immediate importance and represents a broad threat to staff members, the priority is to disseminate as quickly and widely as possible. Traditional security communication methods, such as a communications tree, can be effective in these scenarios, but many organisations now also use broadcast or group messaging. These methods allow for rapid dissemination of critical information, ensuring that all relevant staff are informed and can take appropriate action without delay.

### Examples of a triage information-sharing system

- **Operational importance.** A protest outside the country's parliament buildings is turning violent. Inform staff to avoid the area. Use SMS, a communications tree, broadcast or WhatsApp/Signal group to quickly disseminate information to staff working in the area.
- **Situational update.** Protests are planned in the next few days outside of the parliament buildings. Send out an email advisory and/or incorporate into sitreps, specific security reports and SOPs.
- **Context shift.** Protests brought in a government that is hostile towards humanitarian organisations. Incorporate information as relevant into security reports, briefings or training, and feed into security analytical processes.

### Communications tree

A communications tree is a hierarchy system used to quickly disseminate information to a large group. It begins with one person contacting key individuals, who then each inform others, creating a cascading effect until everyone is reached. This model is ideal for emergencies or urgent updates, ensuring rapid communication. Communications trees can be manual, involving direct calls, or automated, using software to send messages via calls, texts and emails.

For communication at the operational level, introducing redundancy is essential. This means that staff have access to multiple, independent methods of communication, such as radios and satellite phones, so that communication can continue even if one method fails.

- ▶ See Chapter 6.1 for more on different communication methods and developing communication plans that introduce redundancy.

For situational updates or shifts in context that do not require immediate action but have longer-term implications, a more measured approach is often appropriate. These types of updates should still be communicated promptly, but the emphasis should be on providing a thorough analysis of the situation and its potential impact on the organisation's security risk management.

High-level strategic updates might be best communicated through formal reports or executive briefings, while operational updates could be disseminated via more informal channels such as team meetings or group chats. More in-depth concepts and security information could be shared in briefings and training sessions. The key is to ensure that the communication method aligns with the urgency and importance of the information, as well as the preferences and habits of the intended audience.

### Dashboards and apps

Aid organisations are increasingly using dashboards and customised mobile apps to share security information.

Dashboards provide a platform for staff to access security-related information, such as security plans, often in visually engaging ways (such as heat maps) (see *Chapter 3.4 for more on dashboards*).

Mobile apps can deliver real-time security updates, enable rapid incident reporting and offer guidance on specific security situations (such as actions to take at checkpoints). They can also include emergency contact information. Apps can be particularly useful for staff who need access to security information on the go.

### Verification and prudent overreaction

The accuracy and reliability of security information are of paramount importance. There is, of course, an expectation that all information disseminated by the organisation has been verified to the best extent possible. However, in rapidly evolving situations it may not always be feasible to fully verify information before it needs to be communicated. In such cases, the concept of prudent overreaction comes into play.

Prudent overreaction involves taking precautionary measures based on the available information, even if it has not been fully verified, provided that the potential risks justify such an approach. For example, if there is an unverified report of an imminent security threat in a particular area, it may be prudent to temporarily suspend operations or advise staff to take shelter until more information becomes available. The key is to communicate the information in a way that clearly outlines the reasons for the measures taken, while acknowledging the uncertainty surrounding the situation. When conveying such information, it is essential to anticipate likely questions staff might have, such as ‘Why do I need to know this?’ and ‘What do I have to do?’. By addressing these questions upfront, organisations can help reduce confusion and ensure that staff are prepared to take the necessary action in response to potential threats.

### Continuous review and adaptation

Effective security communication within aid organisations relies heavily on continuous feedback and adaptation. Security staff should actively seek and incorporate feedback from colleagues to ensure the information provided is both clear and useful. As security environments and threats evolve, so too must the communication strategies and methods used. Regular reviews or audits of these practices, involving input from all organisational levels, are essential. Staying informed about new communication technologies can help improve the efficiency and reach of security updates.

### Further information

**Persaud, C.** (2022) *Storytelling for learning: using engaging, ethical stories for effective security training*. GISF (<https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/>).