

gisf



Integrated Emergency Communications

Ensuring continuity and
wellbeing in critical incidents

About the Global Interagency Security Forum (GISF)

The Global Interagency Security Forum (GISF) is a member-led NGO forum that works to strengthen the safety and security of aid workers globally. GISF drives collaboration among key stakeholders, strengthens security risk management capabilities, influences global policy, and equips NGOs with the specialised resources, evidence, and tools to effectively manage security risks. With its membership of over 150 NGOs, GISF bridges the gap between operational realities and high-level policy discussions, ensuring aid workers can deliver life-saving assistance in even the most challenging environments.

Overview

Emergency communications work best when the systems are reliable and the messages are human. Integration means planning for both: having backup ways to communicate, and communicating in ways that help staff stay calm and feel supported during critical incidents. This guide sets out an integrated approach to emergency communications for national NGOs. The approach recognises both the technical and human dimensions of effective communications systems during periods of insecurity or as a result of incidents. The guide provides:

- Clear principles for emergency communications, including maintaining redundant communication channels, protecting sensitive information, and regularly reviewing and adapting protocols as operating contexts evolve, while placing people at the centre of these practices;
- Options for selecting infrastructure and systems that achieve redundancy by having main and backup channels and use a mix of tools and processes, so communication continues even if one method fails; and
- Practical advice on integrating simple wellbeing checks into existing emergency and security communications. Throughout, the focus is on people-centred approaches, while remaining aligned with security risk management and duty-of-care responsibilities.

Intended Audience

This guide is designed for national NGOs and focuses on communication systems for staff safety and operational continuity. While international NGOs may draw on global systems or infrastructure, national NGOs often prioritise solutions that are locally accessible, cost-effective, and sustainable in their specific contexts. Their staff often face higher local risks but can also rely on existing community networks, which can support continuity when formal channels fail. Redundancy strategies therefore focus on practical, resilient approaches that combine technical tools with clear procedural methods, ensuring communication remains effective even under challenging conditions.

This guide does not cover communication with communities and accountability to affected populations, though that remains important and should be addressed through complementary systems outside the scope of this guide.



Contents

Introduction	4
1. Principles for Emergency Communications	5
2. Security Communications Systems and Redundancy	7
Additional communication options and systems design	8
Implementation tips and reminders	9
3. Wellbeing Considerations	10
Integration with regular communications	11
Low-intrusion wellbeing check questions	11
Respecting staff networks	13
Duty of care vs. autonomy	14
Practical implementation tips	15
4. Conclusion	15
Useful resources	15

Suggested Citation

Global Interagency Security Forum (GISF). 2026. Integrated Security Communications: Ensuring continuity and wellbeing in critical incidents.

© 2026 Global Interagency Security Forum

This guide is made possible by the generous support of the European Union.



**Funded by
the European Union**



Introduction

Clear, dependable communication is central to effective security risk management, particularly for organisations and frontline workers operating in complex or hazardous environments. During incidents or sudden-onset crisis, one of the first actions is to communicate with and account for staff.

This requires reliable telecommunications infrastructure and systems that support communication before, during, and after incidents. Mobile alerts and check-in calls support rapid information sharing and confirmation of staff safety, but systems alone are not enough. It also requires effective emergency communications procedures, outlining what to say, when to say it, and how to say it in a crisis. Effective emergency communication must also recognise the psychological impact of incidents and support staff wellbeing during periods of stress and uncertainty.

Well-designed emergency communication procedures integrate technical systems, clear processes, and wellbeing considerations. They ensure that critical messages reach staff reliably while also supporting their safety and mental resilience. During an incident, staff are not only recipients of support but also vital sources of timely, accurate information. By maintaining multiple contact channels and embedding simple, routine wellbeing check-ins, national organisations can sustain connectivity and situational awareness under adverse conditions. This strengthens coordination, improves decision-making, and reinforces their duty of care.

Useful vocabulary

Communications tree: A phone, text, email, and social media distribution list for all stakeholders and individuals that may need to be contacted in a crisis. It should have a clear indication of who is responsible for contacting each group or person on the list, and in which format. This allows information to be cascaded down the tree rapidly.

Duty of care: The moral and, in many cases, legal obligation of an employer to provide a reasonable standard of care towards its personnel, and to mitigate, or otherwise address all foreseeable risks that may harm or injure its employees, those acting on its behalf, or for whom it has a level of responsibility.

Government monitoring: Host/donor governments actively engaging in overt or covert observation of organisations' activities, reports, and communications.

Humanitarian telecommunication: The use of communications technologies for the purposes of saving lives, alleviating suffering, and protecting the dignity of crisis-affected populations. This includes technical capacity building, information collection and dissemination, preparedness activities, and/or data analysis.

Security plan: Key documents that outline the security and safety measures and procedures in place, and the responsibilities and resources required to implement them.

Resilience: The ability to anticipate, prepare for, respond, and adapt to incremental change and sudden disruptions. This can be on an individual, team, or organisation level.

For more definitions of key terms, visit the GISF Glossary. Available in Arabic, English, French, and Spanish.



Principles for Emergency Communications

Strong organisations keep people safe by communicating early and clearly. They make sure everyone knows their role and when to raise concerns. They use backup options to stay in touch, protect sensitive information, and regularly update their procedures as situations change. Most importantly, they put people first. They build trust, respect cultural and local differences, and support psychological safety. Every interaction is a chance to reassure someone, gather useful information, calm a situation, and strengthen a positive security culture.

The following emergency communication principles reflect these ideas.

1. People first, always

“Before gathering information, check in on people.”

- **Duty of care:** Communications exist to reduce harm and support people, not just to transmit updates.
- **Psychological safety:** Tone and language matter. Alerts and check-in messages should be framed in ways that provide reassurance and support (“Are you safe?”) as much as instructions on what to do.
- **Confidentiality & consent:** Share only what is necessary; protect identities and dignity, and respect individuals’ right to control their personal information.

2. Human connection under pressure

“Talk to people, not systems.”

- **Human connection:** Use voices and engage known contacts wherever possible. Peer-to-peer communication strengthens trust, shows empathy, and provides opportunities for questions, not just one-way broadcasts.
- **Cultural norms:** Feel free to work within norms that work for you, don't feel obliged to try and replicate the systems you observe international NGOs (INGOs) use. Avoid overly technical or institutional language. Direct human interaction also allows you to gather contextual information and ensures that messages are relevant and sensitive to circumstances.

3. Clarity enables action

“Say what matters, simply.”

- **Clarity:** Use short, plain-language messages that avoid jargon, acronyms or overly technical terms that may confuse or overwhelm people in crisis. Give clear actions: what to do, when, where, and who to contact. Separate facts from what is still unknown.
- **Predictability:** Tell people when the next update will come. Have predetermined check-in schedules (e.g., daily/weekly) and communicate deviations in advance whenever possible. Predictability increases safety and reduces uncertainty in crisis response.

4. Fast escalation, not perfection

“Pass on information early, even if it’s incomplete.”

- **Rapid escalation:** Early warning saves time and lives. It is better to share partial information clearly marked as unconfirmed. Avoid the fear of “getting it wrong”, delaying communication, and use simple escalation triggers everyone understands.

5. Reach everyone, even when systems fail

“If one channel fails, another must work.”

- **Accessibility & inclusivity:** Choose channels that work locally (SMS, radio, in-person, messengers). Consider literacy, language, and connectivity: messages should reach everyone, regardless of language, literacy, disability, or technology access.
- **Redundancy:** Always have a backup method to ensure functionality even during infrastructure disruptions. Test them regularly to ensure they function under stress.

6. Personal responsibility enables collective safety

“Say what matters, simply.”

- **Personal responsibility:** Safety is a shared responsibility. Encourage individuals to prepare phones, contact lists, and contingency plans. Ensure everyone knows:
 - » Who to contact
 - » How to escalate
 - » What to expect in an emergency
- **Responsiveness:** When individuals take responsibility for their own preparedness, when they report incidents promptly, respond quickly to check-ins, and they follow agreed procedures, support can be mobilised without delay.

7. Accountability builds trust

“Build trust: say what you will do - and do it.”

- **Accountability:** Follow through on updates and promises, and acknowledge mistakes or delays honestly. Ensure that roles, responsibilities, and protocols are clearly defined and known to staff.
- **Reporting and feedback:** Keep records simple but consistent and allow for systems and processes that encourage two-way communication.

8. Learn together, improve together

“After action, reflect as people, not just systems.”

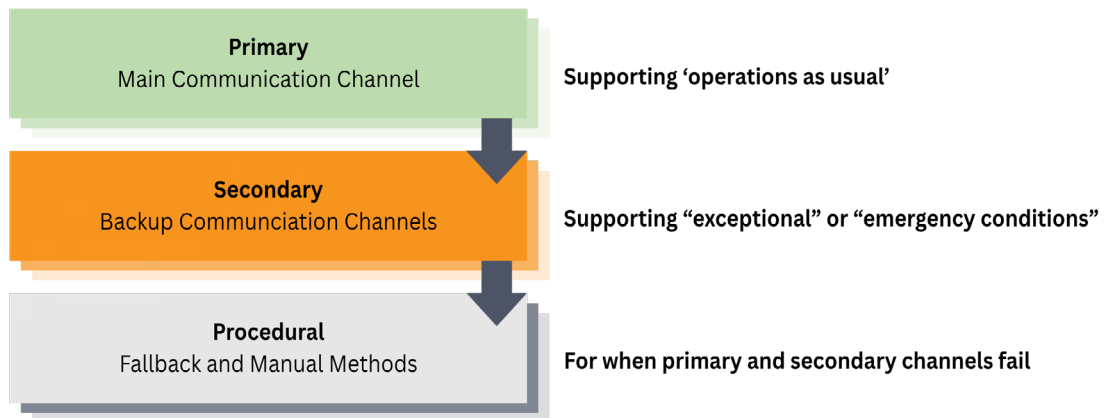
- **Continuous improvement:** Debrief with the whole team, not only management. Capture human lessons (stress points, confusion, emotional impact) and update tools and processes based on incident learnings and lived experience.
- **Close the loop:** Tell teams what changed because of their input.

2

Security Communications Systems and Redundancy

Security communications systems (SCS) are the tools, platforms, and structures an organisation uses to manage security information and communication. These may include check-in/tracking systems, call trees and contact databases, mass notification systems, incident reporting platforms, secure messaging channels, mobile, radio, or satellite networks. Each component of this infrastructure - or system - that supports communication before, during, and after incidents has independent vulnerabilities. Power outages, network congestion, device failure, or human error can all disrupt primary methods at the exact moment they are needed most. It is important that the system as a whole can continue to function, even if some parts may fail.

Redundancy is created by intentionally layering multiple, independent communication paths such as mobile phones, landlines, messaging apps, radios, and predefined in-person or offline protocols, so that if one method fails, others remain available. It also includes having backup contact lists, alternative escalation routes, and shared expectations about which channels to try next if contact is not made. This approach reduces single points of failure, supports faster coordination, and helps teams stay connected during high-pressure situations.



For many national NGOs, redundancy may focus on accessible, low-cost, and locally maintainable solutions rather than specialised infrastructure. The emphasis is on multiple simple options, clear procedures, and staff confidence, so that solutions that can function even when resources or technology fail.

Mobile phones are the most commonly used and familiar means of communication and will often serve as the primary channel during routine operations. However, their reliability is highly dependent on the operating environment. As a minimum standard, at least two independent communication options should be available in each operational area, one of which does not rely on public mobile phone networks.

- **Primary option** (supporting "operations as usual"); and
- **Backup option** (supporting "exceptional" or "emergency conditions" where the primary SCS has failed or is no longer available).

It may be useful to categorise the operating environment using the following scenarios (A, B, or C), to determine the viability of mobile networks, and then consider which communication systems are most appropriate.

Scenario	What this means	Possible options
A. Full availability of mobile phone networks.	The area is adequately covered by a mobile network infrastructure that is reliable and has sufficient built-in redundancies.	Primary: Mobile phones. Back up: Satellite phone or handheld VHF/UHF radios held at site or organisational level.
B. Mobile phone networks are available, but unreliable.	Mobile networks support day-to-day operations but are prone to disruption due to overload, natural hazards, infrastructure failure, or political events.	Primary: Mobile phones. Back up: VHF/UHF radios or limited satellite phones, supported by clear escalation timelines and offline contact lists.
C. Reliable mobile phone networks are unavailable.	Mobile network coverage is insufficient or not dependable for operational and security communications. The organisation cannot rely on public networks during emergencies.	Primary (non-public): VHF/UHF radio network linking staff, offices, and vehicles. Back up: Satellite phones for escalation and external communication, plus defined procedural backups.

Additional communication options and system design

Wide area vs local communications

- **Wide-area systems** (e.g. mobile networks, satellite phones) support escalation, coordination across locations, and external contact.
- **Local systems** (e.g. VHF/UHF radios, mesh networks) enable fast, on-the-ground response where the nearest colleague is often the first responder.
- **Most contexts require both**, with clear guidance on when to use each.

Multiple carriers and SIM cards

- **Using SIM cards from different mobile network providers** reduces dependence on a single operator. This is a low-cost redundancy option where public networks are generally available.
- **Devices should be clearly labelled** and staff trained on when to switch.

Fixed and semi-fixed infrastructure

- Landlines, office-based radios, base stations, or repeaters can provide stable communication points.
- These systems are valuable anchors but must not be the sole option, as they are location-dependent.

Messaging applications

- SMS or low-data messaging apps (e.g. WhatsApp, Signal, Telegram) can support check-ins, alerts, and coordination.
- Messaging should complement, not replace, voice communications in emergencies.
- Clear guidance should exist on appropriate use, escalation triggers, and limitations.

Remember: Using a messaging app as your 'backup' communication channel does not provide redundancy. These apps depend entirely on public mobile or internet networks, so if the mobile network fails, messages stop flowing.

Regulatory and government controls

In some contexts, governments may restrict certain telecommunications tools, require registration of SIM cards, monitor communications, block specific platforms, or deliberately implement internet or mobile network shutdowns during periods of tension. Redundancy planning should therefore consider:

- The risk of network-level shutdowns affecting all public mobile and internet services simultaneously.
- Restrictions on specific platforms or encrypted messaging applications.
- Legal implications of using satellite equipment, radios, or encryption tools.
- The possibility that communications may be monitored.

Where such risks exist, systems should combine different technologies (e.g. networks and independent radio systems) and clear procedures for switching when interference occurs. Staff should also understand the legal and security implications of the tools they carry and use. In all cases, ensure power resilience: spare batteries, vehicle chargers, generators, or solar solutions are essential to sustaining all communication systems during prolonged disruptions, including deliberate network shutdowns.

Implementation tips and reminders

The above options strengthen redundancy when they are independent, complementary, and clearly understood by staff. However, redundancy relies not just on systems, but on people. The following tips provide practical guidance on how to implement and use emergency communications in ways that support staff confidence and readiness.

Tips and Reminders

- **Test and practice** communication systems regularly, including backup options, not only the primary system.
- **Train all staff, recognising that emergencies are often managed initially by those closest to the situation.**
- **Keep guidance simple and accessible:** ensure simple escalation procedures are understood by all staff, stating who to contact, when to switch or how to escalate if there is no response, and expected response times.
- **Provide offline access** to contact lists, call trees, and procedures.
- **Establish procedural alternatives:** determine clear escalation paths, secondary contacts, and low-tech options (e.g., runners, in-person check-ins) in case all technical channels fail.
- **Review communication arrangements regularly**, especially after:
 - » Changes in staff or locations
 - » Security incidents or near-misses
 - » Shifts in network reliability or risk context

Having redundancy does not require complex systems. For NNGOs, resilience is achieved by combining simple, independent communication methods, clear procedures, and prepared staff. This layered approach ensures that the loss or degradation of any single channel does not result in a loss of communication, while aligning with local operating realities.



Wellbeing Considerations

While reliable communication systems are essential, they are only one part of effective emergency response. Effective emergency communication is not only about systems and redundancy, but also about the people using them. What, when and how to communicate directly affects staff wellbeing, which in turn affects how people communicate, make decisions, and support one another. Every check-in, message, or conversation is an opportunity to minimise risk through calm, clear, and compassionate communication. Yet in many contexts, mental health and wellbeing discussions can be sensitive or stigmatised.

The following section focuses on practical ways to integrate wellbeing checks into existing security and communication routines, keeping the emphasis on support rather than diagnosis. Subsequent sections explore how to leverage local staff support networks, and how to balance organisational duty of care with respect for staff autonomy and local context.

Integration with regular communications

Routine comms (e.g., check-ins, daily safety calls, radio checks, messaging apps) already serve multiple purposes, namely, to confirm location and security, to track operational status, and/or to identify immediate risks (safety, health, environment).

Wellbeing checks can be built into routine communication without adding burden. These are simple, non-intrusive check-ins focused on safety and support, not assessment or diagnosis. Staff should be reassured that they are never expected to disclose personal mental health information unless they choose to do so.

Key approaches

- Keep it routine, not a sign of trouble. “We ask everyone this”
- Validate feelings: “It’s totally normal to feel that way here.”
- Prioritise local support first (i.e., friends, family, colleagues).
- Goal: To strengthen people, not monitor them.
- Avoid rushing - pauses can create space to share information.
- Respect privacy and culture.
- Consider their emotional state over time (trend = risk).

What to check

- Safety – Are they physically secure?
- Rest – Are they sleeping/eating okay?
- Capacity – Is the workload manageable?
- Support – Do they feel connected to their team?

Low-intrusion wellbeing check questions

On the next page, you will find various questions that allow concerns about hypervigilance, fear, or burnout to surface indirectly.

Daily functioning

"How has your sleep been the past couple of days?"

"Have you been able to take regular meals?"

"How's your energy level today?"

Stress and coping

"What's been the most challenging part of the week?"

"Is there anything adding extra pressure on you right now?"

"What's helping you manage stress best at the moment?"

Emotional state (indirectly)

"On a scale from 1-10, how manageable are things feeling today?"

"Was there a moment this week that felt unexpectedly difficult?"

"If there's one thing that would make tomorrow easier, what would it be?"

Social connection

"Have you had the chance to connect with teammates or friends recently?"

"Who have you been able to lean on when things get stressful?"

Agency and support

"Is there anything you need that you're not getting right now?"

"What can I do today that would be most helpful?"

Situational questions related to high-risk environments

"How safe are you feeling in your current location?"

"Anything in the environment making you uneasy or distracted?"

"Any changes in routine or surroundings impacting your focus or rest?"

Indicators you can listen out for (without asking directly)

- Emotional tone + reduced affect
- Withdrawal or short responses
- Expressions of hopelessness or cynicism
- Difficulty concentrating or remembering operational details
- Comments about risks not feeling worth it anymore

Respecting staff networks

In addition to providing non-intrusive wellbeing checks, many national NGO staff rely on informal or traditional support networks, such as family, community groups, peers, or faith leaders, during times of stress or crisis. These networks are often trusted, culturally appropriate sources of emotional and practical support. Where appropriate and with consent, staff should be encouraged to draw on their own support systems.

At the same time, it is important to recognise that traditional or community networks may, in some circumstances, contribute to harm, exclusion, or increased risk. In such cases, organisations have a duty of care to respond appropriately, including offering alternative support and escalating concerns where safety, safeguarding, or serious wellbeing risks are identified. Balancing respect for autonomy with duty of care requires careful judgement, cultural awareness, and a focus on prevention of harm.

Do

- **Encourage staff** to draw on trusted local networks (family, peers, community, faith leaders) for support.
- **Ask for consent** before engaging or involving anyone outside the team.
- **Acknowledge and respect** cultural, religious, and social norms in how support is offered.
- **Offer organisational support** as a complement, not a replacement, to local networks.
- **Maintain open communication** and check for safety or wellbeing concerns.
- **Escalate or provide additional support** if a staff member's safety or wellbeing cannot be met through local networks alone.

Don't

- **Assume** organisational intervention is always preferred or primary.
- **Pressure staff** to use formal organisational support if they prefer local networks.
- **Override**, monitor, or control local support structures.
- **Ignore** cultural or religious practices when offering support.
- **Share personal information** without consent.
- **Treat local networks as a substitute** for escalation when safety risks are present.

Duty of care vs. autonomy

In emergency communications and wellbeing checks, NGOs must support without controlling and offer care without intruding. This tension is particularly acute for national staff, who:

- Often remain embedded in the affected community after an incident.
- May already have strong family, community, and faith-based support.
- May not view organisational involvement in wellbeing as necessary or appropriate.
- May face stigma, reputational risk, or social consequences if distress is disclosed.

Duty of care is the legal and moral obligation on NGOs to take reasonable steps to prevent foreseeable harm to individuals and to respond appropriately when harm occurs. This requires maintaining open lines of communication, offering assistance without pressure, and clearly explaining what the organisation can and cannot provide.

Autonomy recognises the right of individuals to make their own decision about their own wellbeing, support systems, and personal lives. It is important to respect staff as capable professionals with their own support networks, ensuring organisational systems complement rather than monitor, replace, or override them - while remaining attentive to situations where additional support or escalation may be necessary.

What duty of care requires you to do

- Check on staff safety and immediate wellbeing after incidents.
- Provide clear information, reassurance, and predictable communication.
- Identify indicators of acute distress that could affect safety or work.
- Offer access to support (organisational or external).
- Escalate where there is foreseeable risk to life, health, or security.

What duty of care does not require you to do:

- Diagnose or manage mental health conditions.
- Monitor private emotional states.
- Replace personal or cultural support systems.
- Force staff to engage with organisational support.
- Maintain responsibility for long-term mental health outcomes.

Boundaries matter. Crossing them can undermine trust and autonomy, so it is important to recognise colleagues' right to manage their own wellbeing and support networks. That said, there are limited but important circumstances where duty of care must take precedence, including:

- Risk of self-harm or harm to others.
- Serious impairment affecting safety or decision-making.
- Legal, safeguarding, or child-protection concerns.
- Repeated exposure to traumatic incidents without recovery time.

Even then, escalation should be proportionate, clearly explained, respectful of dignity, and focused on safety, not control.

Practical implementation tips

Do

- **Integrate with existing comms windows:** don't create separate check-ins just for wellbeing.
- **Keep questions neutral & functional:** safety, sleep, energy, social support, workload.
- **Track trends, not single data points:** spot deterioration early without making anyone uncomfortable.
- **Offer multiple support channels:** peer support, supervisors, optional professional support.
- **Document protocols clearly:** staff understand what will happen with their responses, maintaining trust.



Conclusion

Emergency communications are not only a technical or procedural function; they are human interactions that carry real impact at moments of stress and uncertainty. Effective emergency communication therefore relies on the seamless integration of human and technical elements. Well-designed systems combine robust, redundant channels with attention to staff wellbeing, recognising that people are both critical recipients and providers of information.

Technical infrastructure ensures messages are reliably delivered, while human-focused practices, such as non-intrusive wellbeing checks, support resilience, situational awareness, and decision-making under pressure. When these elements work hand in hand, organisations strengthen their duty of care, maintain connectivity in adverse conditions, and enhance coordination and response effectiveness, demonstrating that successful emergency communication is as much about people as it is about technology.

Useful resources

[GISF. \(2020\). *Security to Go*](#)

[Humanitarian Practice Network. \(2025\). *Good Practice Review 8: Chapter 6.1 Managing information and communications security*](#)

[UNHCR. \(2024\). *UNHCR Emergency Handbook: Mental Health and Psychosocial Support \(MHPSS\)*](#)

[UNSMS. \(2021\). *Security Management Operations Manual, Chapter XVII Guidelines on Security Communications Systems*](#)

gisf



Global Interagency Security Forum

GISF Research and Programmes
E: research@gisf.ngo

www.gisf.ngo