EMERGENCY COMMUNICATION STARTS BEFORE THE INCIDENT

What organisations should prepare to communicate during the first 72 hours of an emergency.



STEP 1

PREPARE BEFOREHAND

Know who leads, what could happen and who you need to reach, before an emergency forces the question.

1 Establish your emergency response team

- [ ] **Appoint a multidisciplinary team.** Include leadership, operations, communications, HR and IT/security. Smaller organisations can combine roles.
- [ ] **Assign named responsibilities and substitutes.** Define who leads the response, verifies information, approves messages and contacts stakeholders.
- [ ] **Keep an accessible contact list.** Include alternative contact methods and a protected offline copy.

2 Identify and assess potential scenarios

- [ ] **List relevant your business emergency.** Consider power outages, floods, cyberattacks, health emergencies, security incidents, armed conflicts, terrorist attacks and major service disruptions.
- [ ] **Assess likelihood and severity.** Evaluate risks to people, operations and essential services.
- [ ] **Define activation triggers.** Establish when the dedicated communication team must respond and when emergency communications begin.

3 Map your stakeholders and their risks

- [ ] **Identify affected groups.** List all stakeholders who could be affected by the emergency, such as employees, customers, partners and donors.
- [ ] **Assess the impact on each group.** What risks do they face, what information do they need and what actions might they have to take?
- [ ] **Prioritise vulnerable and highly affected stakeholders.** Consider accessibility, language and communication barriers.

STEP 2

PLAN YOUR COMMUNICATION ROADMAP

During an emergency, your team should not be deciding from scratch who communicates, what to say or which channels to use.

4 Establish communication procedures

- [ ] **Assign communication roles.** Define how collects facts, drafts, approves and delivers messages, including an urgent approval route.
- [ ] **Identify reliable information sources.** Agree how facts will be verified internally and against instructions from competent authorities.

5 Prepare stakeholder-specific messages

- [ ] **Draft templates for priority scenarios.** Cover closures, service disruptions, cancellations, temporary arrangements, reopening. Include messages for data breaches, product recalls, public allegations.
- [ ] **Tailor messages to each stakeholder group.** Explain what happened, how they are affected, what to do and where to get help. Specify what your organisation is doing to mitigate the emergency's damage.
- [ ] **Pre-approve templates and procedures.** Incident-specific facts must still be verified before messages are sent.

Emergency message template

- **Situation:** What has happened? (Verified facts)
- **Impact:** Who is affected and how?
- **Action:** What are you doing to limit the impact?
- **Support:** How does your organisation support recipients, and where can they get assistance?
- **Next update:** When and through which channel?

6 Document and test your plan

- [ ] **Create a written emergency communication playbook.** Include contacts, responsibilities, scenarios, stakeholder priorities, and message templates.
- [ ] **Prepare a step-by-step activation roadmap.** Make it accessible to authorised staff, including offline.
- [ ] **Run simulations.** Test responsibilities, backup channels, and approval procedures. Update the plan regularly.

STEP 3

RESPOND, UPDATE & RECOVER

When an emergency occurs, activate the plan you have already prepared.

7 Activate and verify

- [ ] **Convene the emergency response team** and confirm immediate responsibilities.
- [ ] **Verify the situation** using reliable internal sources and official warnings, including LU-Alert where relevant. Follow applicable safety instructions.
- [ ] **Identify and contact affected stakeholders,** prioritising people who need to act immediately.

8 Communicate quickly and responsibly

- [ ] **Activate prepared messages.** Adapt templates to verified facts and stakeholder needs.
- [ ] **Provide clear, timestamped updates.** State what is known, what people should do and when the next update will follow.
- [ ] **Pause inappropriate marketing.** Review scheduled posts, advertising, newsletters and automated messages.

YOUR CLAIMS SHOULD NEVER BE STRONGER THAN YOUR EVIDENCE

Communicate what you can verify. Explain what is still uncertain. Promise safety, recovery, or reopening times only when you have reliable confirmation.

9 Maintain communication during the first 72 hours and beyond

- [ ] **Coordinate updates across channels.** Keep stakeholders informed.
- [ ] **Monitor questions and misinformation.** Correct inaccurate information and protect privacy and sensitive details.
- [ ] **Communicate service changes.** Explain what remains available, what is suspended and what alternatives exist.
- [ ] **Continue updates as long as needed.** The first 72 hours are not a deadline for ending communication.

10 Recover and improve

- [ ] Inform stakeholders when normal operations can safely resume.
- [ ] Review the situation before restarting regular marketing.
- [ ] Document lessons learned and update the communication plan.

BEFORE SENDING ANY MESSAGE IN A CRISIS SITUATION

- [ ] **Are the facts verified?**
- [ ] **Is the message relevant and actionable?**
- [ ] **Is it consistent with official instructions?**
- [ ] **Does it protect people's safety and privacy?**
- [ ] **Is the next update or contact clearly indicated?**



Preparation makes communication possible when time is limited

Book a short consultation with KOLO to review your crisis playbook or prepare your team before an emergency occurs.

The checklist provides communication recommendations and does not replace official instructions, safety requirements, or legal advice.

Prepared by KOLO info@kolo.lu www.kolo.lu

kolo Communication for Impact