

Dozens of pages of technical information and difficult-to-understand terms that have been forgotten in a folder hidden in the far corner of a closet. This is not the kind of security policy you should adopt in your organization, nor is it the type of document we will be discussing today. Together with Joseph Hamood, the safety and risk manager at International Media Support, **we will explain how to create a simple, applicable, and effective security policy for your newsroom.**

## Joseph Hamood

Safety and Risk Manager,  
International Media Support



### How to introduce the concept of security to our team without causing panic?

We need to explain to the team that security is necessary for us to continue our operations in any situation. To do so, we must understand what would prevent us from doing so. It is crucial to link risks and security to business continuity because that is the primary reason for developing such a policy. The document should indicate which threats to focus on and how to address them.

### How is a security policy created?

The biggest risk with security policies is that they are too long and difficult to understand. Simply hiring someone to produce a document that will only be kept on the shelf and occasionally shown to donors does not solve the problem. **A security policy should be a useful, practical tool**, not a bureaucratic formality. The size of the policy is not as important as the fact that it is ours. We can adjust it as the organization evolves. Monitoring and reviewing the policy can be an annual team exercise.

First, we will gather the entire team to identify threats to our work and our ability to continue operations. It is crucial that these risks reflect our reality rather than the assumptions of outsiders. This discussion must be honest and reveal our genuine concerns. These risks may include management issues, internal conflicts, external attacks, the political situation, or legal problems. Even if some of these issues are sensitive, we must be aware of them and address them; otherwise, they will continue to grow and may eventually lead to a crisis.

First, we identify what could affect our work. Then, we prioritize them according to how urgently they need to be addressed. Then, we look for the right solution for each issue so that we can manage them effectively.

The next step is to identify other stakeholders. Whatever problems we discover, we should know that we are not alone. It is important to understand who our allies are and what role they play. It is also important to establish relationships with them and talk to them before a crisis occurs.

We also need to consider ethical and moral issues, such as duty of care and gender inclusion, which we may have initially overlooked. Next, we will develop a contingency plan for the most urgent risks.

The most important aspect of this process is that it reflects the team's work, making the process and results much more relevant. These are our ideas on how to protect our organization. In this way, the policy becomes practical and grounded in reality.

The purpose of policy is to prepare us in advance for potential threats because only through preparation we can ensure organizational continuity.

### When is the best time to work on our security policy?

We definitely need to do this while things are calm. We cannot prepare while we are fighting; planning must be done before the crisis. The essence of preparation is to be able to respond proactively, not reactively.

### Do we need a guide on how to implement the policy?

Yes, you need a guide, but not an expert who will create policies for us or provide templates for us to copy and paste. The risk analysis process covers five key areas: operational, political, legal, financial, and reputational. The team will discuss each of these areas, and the guide can provide direction or feedback.

### Who is on the crisis management team?

When selecting a crisis management team, it is important to choose individuals who are familiar with the organization and its internal processes, regardless of their position. We also need technical people. Here, we disagree with the above point of view because IT experts do not need to be part of the organization in this case. They can assist with a specific task without being part of the crisis management team.

Similarly, we can call on an external expert for general consulting in emergency situations. This does not mean that the size of the crisis team will increase. It will continue to consist of key people from the organization. However, we will also have a few additional contacts that we can activate if necessary.

The crisis team is formed after analyzing and assessing the risks, based on the identified conclusions and needs. Only then will we know how many people are needed and which external personnel to call upon.

### What happens after a crisis?

After a crisis, we analyze what happened, what could have been done better, which strategies proved useful, which tools we used, and how we need to update our policy. We will always find gaps because crises are dynamic. No matter how prepared we are, there will always be blind spots.

### How much crisis information should we provide to our employees, collaborators, and the public?

There are managers within the team who oversee the crisis, as well as people who are affected by it. We need to identify those who may be affected and adapt our communication strategy accordingly.

Team members who are not directly involved in crisis management but who are affected by it must be informed of relevant issues so they can make informed decisions. For example, if there is a cyberattack or office raid, the team should be told to stay home. We need to implement a communication strategy so that the team receives regular updates (daily, every other day, or less frequently depending on the situation). The public, on the other hand, does not need daily updates. A public announcement explaining what happened, how it affects us, and which services are changing may be sufficient.

Therefore, an important step in risk analysis is analyzing the partners involved and their relationship to the risks.

### How can we create a budget that allows us to respond promptly to security needs?

This is the case when safety and crisis preparedness intersect with organizational development. All plans for ensuring operational continuity should be included in the development budget.

Our partners will play an important role here. We need to communicate to them that this investment in security and continued development is important to us. For instance, developing IT infrastructure not only provides protection; it also means we are investing in the organization's resilience and capacity. It's not just a security issue; it's a necessity for organizational development.

In real crisis situations, additional support will be available from various sources. If we have plans in place and know exactly what we need, we will be able to respond quickly with precise requirements.

So, we have the development budget, on the one hand. And, there are emergency situations for which we will access emergency funds, on the other hand.



#### Opportunity!

Newsrooms can apply for grants to build institutional capacity. Eligible activities include initiatives that strengthen digital security and those that prevent burnout and support the mental health of editorial teams. Click [here](#) for details.



#### Get Help!

If you are experiencing ongoing stress and anxiety, you can request a free and confidential consultation with a psychologist using [this chatbot](#) or by filling out [this form](#). You will be connected with a specialist within 48 hours.

**If you liked what you read, please recommend our newsletter to a colleague. Feedback helps us get better. Let us know what you think about the newsletter at [api@api.md](mailto:api@api.md).**

