open briefing

Prevent

Ensure that your foundation is properly prepared to support its grantees

#1 Engage **retained providers** to support the security and wellbeing of both your own staff and targeted grantees.

#2 Monitor the **social and political contexts** of your programmes for signs of deterioration that might impact grantees' safety due to their location or profile.

#3 Provide programme staff with regular **training** in security risk assessments, digital security, Psychological First Aid, and vicarious trauma.

#4 Create a **crisis management** team and ensure that they have a crisis management procedure and receive regular crisis management training.

#5 Develop and implement **policy frameworks** for security risk management, information security, and staff wellbeing.

Encourage grantees to think about holistic security throughout their grant journey

#1 Explicitly include holistic security and risk management in any **pre-award discussions** with potential grantees.

#2 Include safety and security, digital security, and wellbeing and resilience as separate lines in any application **budget templates**.

#3 Ensure that grantees are aware of the **support and resources** that you *will* and *will not* be able to provide in a crisis.

#4 Offer regular **training** to your grantees in security risk assessments, digital security, wellbeing and resilience, and Psychological First Aid.

#5 Periodically **share best practice** and useful tools with grantees.

Open Briefing prevents and responds to serious attacks on the people and organisations fighting for peace, human rights and environmental justice around the world, and works to create the conditions in which they no longer happen.

We also provide consultancy, training, and retained support to help nonprofits and foundations understand and meet their risk management and duty of care commitments to staff, grantees, and local partners.

open briefing

Respond

#1 Ensure immediate safety

- What is their current location? Are they safe there?
- Do they need medical attention?
- Do they need legal representation?
- Can a local trusted third party safely check on them?
- Does an embassy or other diplomatic representation need alerting?
- If appropriate and safe, do local law enforcement need to be involved?
- If a staff member is involved, have you contacted your foundation's insurance provider?

#2 Address wellbeing

- Help them to feel calm.
- Do not ask them to relive traumatic events, but listen if an account is offered.
- Allow those affected to make decisions for themselves, but discourage unnecessary risk taking.
- Help them with practicalities and encourage them to maintain their usual routines of eating, sleeping, and exercise.
- Be prepared to repeatedly refocus them on next steps and on specific, practical tasks.

#3 Establish reliable communications

- Confirm a secure messaging app to use (e.g. Signal).
- Encourage them to follow the digital security guidance at https://protocol.openbriefing.org.
- Obtain or update their full range of contact details.
- Get the contact details of local trusted third parties who can physically check on them if you lose contact.
- At the end of each contact, agree the next time that you will talk.

#4 Gather information

- Record the Who? What? When? Where? Why? How? of any incident.
- Seek to understand both the *intention* and *capability* of any adversary or attacker.
- Identify the grantee's ability to respond, available resources, and local and international allies.

#5 Develop a plan

- Based on the threat and your and the grantee's abilities to respond, can this be dealt with at the programme level or do you need to **escalate** (internally) or **refer** (externally)?
- Co-design a plan with the grantee and other stakeholders that includes:
  - **Goals:** Agree the desired outcomes for the short, medium, and long term. Focus on the short term.
  - **Levers:** Identify the allies and resources that can be leveraged to achieve the goals.
  - **Contingencies:** Plan what to do if things go wrong or deteriorate. Document these plans.

Remember: Your job is to triage and provide a support role only. So respond appropriately and gather information, then formulate a plan and escalate or refer as required.

To the fullest extent permitted by law, Open Briefing will not be liable for any loss, damage or inconvenience arising as a consequence of any use or misuse of this resource.