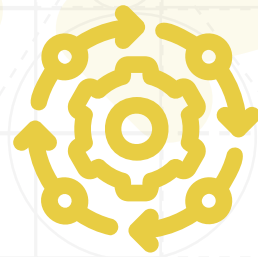Survivor Engagement Safety Plan
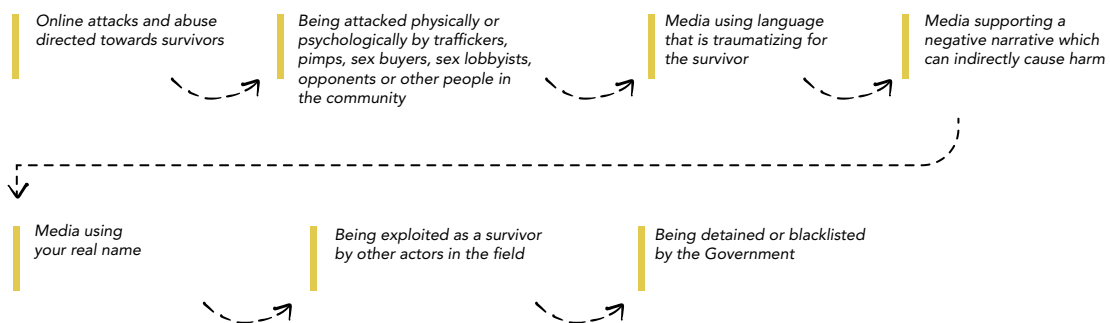
Safeguarding survivor-led organizations

WHAT DOES IT MEAN TO SAFEGUARD SURVIVOR-LED ORGANIZATIONS?

For a survivor-led organization, safety and protection means creating an environment where survivors feel secure, respected, and empowered. It involves implementing robust security measures to safeguard survivors and their sensitive information, ensuring confidentiality and trust. Being safe and protected also entails fostering a culture of inclusivity, where survivors' voices are valued, and their autonomy is upheld. Additionally, it involves offering comprehensive support services tailored to survivors' needs, including emotional, physical, economical and legal assistance. Ultimately, safety and protection for a survivor-led organization means prioritizing the well-being and agency of survivors in all aspects of the organization's work.

This guide is developed by Beyond Survivors in cooperation with Protection International. Beyond Survivors is a cluster of survivor-led organizations and its overall goal is to strengthen, structure and safeguard survivor engagement in the field of trafficking and exploitation of children. For more information please visit www.beyondsurvivors.org.

Common threats faced by survivors

Online attacks and abuse directed towards survivors

Being attacked physically or psychologically by traffickers, pimps, sex buyers, sex lobbyists, opponents or other people in the community

Media using language that is traumatizing for the survivor

Media supporting a negative narrative which can indirectly cause harm

Media using your real name

Being exploited as a survivor by other actors in the field

Being detained or blacklisted by the Government

Common **threats** faced by survivors

Personal physical harm	*Physical harms extended to family friends, or others*
Psychological harms (personal)	*Psychological risks due to stress, triggering questions, speaking about past trauma, etc*

Risks to survivor-led organizations:

In addition to the general risks faced by survivors who engage in this field which are also a threat to the survivor-led organizations, we have identified specific, more internal risks that survivor-led organizations are often faced with. These include, but are not limited to:

- Lack of capacity: Limited resources, such as funding and staffing, can hinder the organization's ability to provide adequate support to survivors.

- Inadequate governance: Weak leadership and poor decision-making processes can affect the organization's efficiency, accountability and reputation.

- Survivor staff turnover and instability: Mental health challenges and internal conflicts can lead to staff turnover, affecting the organization's stability and credibility.

- Lack of institutional knowledge: Poor documentation and resource constraints make it difficult to ensure continuity and effective decision-making, hindering long-term sustainability.

- Re-traumatization, burnout and vicarious trauma: Staff and volunteers may experience an enormous emotional strain as they are working in a field where they themselves have been exploited in addition to dealing with the past exploitation of their colleagues.

- Data security and confidentiality: Mishandling sensitive survivor information can have grave consequences for the physical and psychological wellbeing of survivors, which could damage survivors' trust in the organization.

- Conflicting interests: Internal conflicts, differing ideologies, or competing interests may compromise the organization's survivor-centric focus.

- Survivors still connected to past exploitation: Survivors still connected to their abusers pose safety risks to the organization and its services. There is also a risk of survivors themselves turning to perpetration and may attempt to exploit the organization for recruitment, undermining its values.

Analyzing Your Context:

Understand the social, cultural, and political environment in which the organization operates, and the forces and actors that oppose or support you.

Drawing a timeline of security incidents and threats:

Document past security incidents and threats faced by the organization and survivors.

Share and analyze security incidents within the organizations.

Identify patterns and trends to inform future risk management strategies.

Determining risk situations:

Consider specific activities, locations and situations where survivors may encounter threats, such as approaching women in exploitation or engaging in public activities such as advocacy.

Apply a gender and intersectional perspective to understand unique vulnerabilities.

Assessing risk level:

Identify the organization's vulnerabilities and capacities in relation to the threats and risk situations.

Reflect on whether dimensions related to gender and intersectionality have an impact on risk.

Consider factors such as the nature of threats, the organization's vulnerabilities, and existing security measures.

Evaluate the likelihood of threats materializing and their potential impact on survivors and the organization: do not only consider the risks in isolation, but in relation to your work objectives too, i.e. is it worth taking this risk to achieve this objective?

Turning vulnerabilities into capacities:

Reflect on how you can turn vulnerabilities into capacities.

Develop strategies to strengthen capacities, such as training of staff and/or members, implementing security protocols or guidelines.

Mobilize supporting actors, such as partnering organizations or community members, to enhance protection measures.

If the risks are still too high after taking additional security measures, ask yourself whether there are alternative ways to achieve your work objectives in a more secure way.

When to analyze risks:

Conduct risk analysis while designing projects and programs to integrate security measures from the outset.

Analyze risks before engaging in activities like approaching women in exploitation, public speaking, or media interventions.

Also, analyze risks after receiving threats or dealing with security incidents to inform future responses and improve protection measures.

Taking security measures:

Register and document threats or security incidents promptly.

Analyze each incident to understand its nature and implications.

Take appropriate security measures, such as enhancing physical security or updating protocols, to mitigate risks and ensure the safety of survivors and staff.

Assessing the objective towards the risk and alternative actions involving less risks:

Considering alternative ways of reaching the same objective if it involves less risks.

Is it worth taking that level of risk to achieve these objectives? Levels of risk vs. sense of achievement.

After assessing risk levels, think about how to mitigate risks and if that's not possible, think about alternative ways in order to achieve your objectives.