EMPHNET
The Eastern Mediterranean
Public Health Network

▶ GHD I EMPHNET: working together for better health

Safety and Security Framework

A PRACTICAL ORGANIZATIONAL FRAMEWORK FOR SAFE, SECURE, AND RIGHTS-BASED HIV PROGRAMMING

Version 1.0

Introduction

Ensuring the safety, security, and dignity of key populations (KPs) is a fundamental prerequisite for effective, ethical, and rights-based HIV programming. In many countries across the Middle East and North Africa (MENA) Region, KPs face complex and intersecting risks, including stigma, discrimination, criminalization, gender-based violence, and breaches of confidentiality. These risks can be exacerbated during the implementation of programmatic activities if not proactively identified and mitigated.

The Safety and Security Framework has been developed to support Sub-Recipients (SRs) and implementing partners in systematically integrating safety and security considerations into all stages of KP and HIV-related activity design and implementation. The Framework provides practical, adaptable tools to help identify, assess, and mitigate risks, while ensuring that activities are conducted in a manner that prioritizes participant protection, confidentiality, and ethical standards.

This Framework is grounded in Global Fund guidance, aligned with GHD|EMPHNET's policies related to safety and security, and informed by regional experience working with KPs in diverse and often sensitive contexts. It adopts a risk-based, participant-centered, and context-sensitive approach, recognizing that safety and security risks vary significantly depending on legal environments, social norms, and the specific vulnerabilities of different population groups.

The Framework is designed as a living and adaptable resource, encouraging SRs to tailor its components to their local context, operational realities, and the needs of the populations they serve. It emphasizes proactive planning, continuous risk assessment, and learning from participant feedback to strengthen programming over time.

Specifically, the Framework includes a set of complementary tools, guidance documents, and adaptable resources that SRs can use, adapt, or build on based on their organizational context, existing systems, and programmatic needs. The Framework is not intended to replace existing organizational systems, but rather to complement and strengthen them where needed.

By using, adapting, or integrating relevant components of this Framework, implementing partners can:

- Enhance the safety and protection of participants and staff
- Strengthen trust and engagement with key populations
- Reduce the risk of harm, exposure, or unintended consequences
- Ensure compliance with ethical standards and donor requirements
- Improve the overall quality, effectiveness, and sustainability of HIV programming

Framework Components and Application

This framework includes guidance and practical tools that may support organizational systems, activity planning, implementation, and review. SRs and implementing partners may use individual components or selected elements based on their needs and existing procedures, and the application of this framework should be reviewed periodically to reflect operational experience, community feedback, and emerging risk.

Depending on organizational needs, capacities, existing systems, and identified risks, SRs may choose to use one or more of the following components:

- The Guidance for SOPs may support SRs in reviewing or strengthening existing organizational procedures and systems.
- The Safety and Security Readiness Checklist may be used to identify strengths, gaps, and areas requiring improvement.
- Post-activity feedback mechanisms, including KP feedback surveys, CRSS findings, incident reports, and other feedback channels, may be used to strengthen future planning and risk mitigation efforts.
- The Participant Safety Briefing Template may support the consistent communication of safety and security information to participants before activities.
- The Security Risk Assessment Matrix can be used to identify and assess safety, security, confidentiality, legal, social, and operational risks and inform appropriate activity planning and mitigation measures.

The framework should be viewed as a living resource that supports continuous learning, risk mitigation, and quality improvement. SRs are not expected to implement every component in full or in the same way, the goal is intentional, context-appropriate strengthening of safety and security practices.

For an SR seeking to strengthen their safety and security practices, the recommended steps are:

1

Conduct a context review
Before engaging with any component, review your operating environment, including the legal context, identified risks to KP participants and staff, existing organizational policies, and any prior safety or security incidents. The Safety and Security Readiness Checklist is a useful starting point for this assessment.

2

Identify gaps and priorities
Use the Readiness Checklist to identify where organizational gaps exist. Not all gaps need to be addressed at once. Prioritize based on your risk profile and available capacity.

3

Develop or adapt an SOP
The Guidance for SOP section provides a recommended structure and components. SRs may choose to develop one comprehensive organizational SOP covering all areas, or separate SOPs for specific functions (e.g., incident reporting, digital security), depending on their organizational size and complexity. Either approach is acceptable, as long as the SOP is realistic, contextually appropriate, and actively used.

4

Implement, collect feedback, and adapt
Conduct activities using the safety protocols established in your SOP. Use the Post-Activity Feedback Question Bank to gather input from participants and use that feedback to continuously improve your safety and security practices over time. SRs are encouraged to revisit and update their safety and security practices regularly, particularly when the operational context changes, new risks emerge or following any safety-related incident.

Alignment with International Guidance and Global Fund Standards

This framework is aligned with relevant Global Fund frameworks as well as normative standards and documents, including:

- Global Fund Strategy 2023–2028
- Global Fund SECURITY TOOLKIT: Protecting implementers and improving program outcomes
- Global Fund Code of Conduct for Recipients of Global Fund Resources
- Global Fund Ethics and Integrity Initiative – Revision 1
- Global Fund 2022, technical brief removing human rights-related barriers to HIV services, allocation period 2023-2025
- WHO Consolidated guidelines on HIV, viral hepatitis and STI prevention, diagnosis, treatment and care for key populations
- Global HIV Prevention Coalition (GPC) Planning and Managing HIV Programmes with Key Populations
- AMAN MENA Security Protections for Organizations Working with Key Populations to Strengthen HIV Programming in the Middle East and North Africa

Guidance for Developing

This section provides guidance for SRs on reviewing, developing, adapting, or strengthening organizational Standard Operating Procedures (SOPs) and related internal systems that support safe, secure, and rights-based implementation of HIV-related activities. Recognizing that many SRs may already have existing policies, procedures, safeguarding mechanisms, or organizational frameworks in place, this guidance is intended to complement and strengthen existing systems where relevant, rather than require the development of entirely new procedures.

The section outlines key components and minimum considerations that may be adapted to fit each SR's organizational structure, operational context, existing systems, and identified risks. Recognizing the diversity and complexity of operating environments, this guidance is intended as a flexible framework rather than a prescriptive approach. SRs may adopt, adapt, expand, or integrate these considerations into existing organizational procedures and systems as appropriate.

Table 1 outlines the recommended structure and minimum components for SR SOPs to ensure safe, rights-based, and accountable implementation of HIV programs. It is intended as a flexible framework adaptable to different operational contexts.

Table 1 Recommended components for SR Safety & Security HIV SOPs

Section	Component	Key Elements / Minimum Requirements
1. **Foundations and Governance**	Human Rights Principles	• Non-discriminatory access to services • Respect for dignity and autonomy • Confidentiality and informed consent
	Code of Conduct	• Ethical behavior of staff • Professional standards • Respectful engagement with communities
	Gender Equality	• Address gender-related barriers to HIV services • Promote equitable access and participation
	Safeguarding PSEAH (Prevention of Sexual Exploitation, Abuse and Harassment)	• Prevention of SEAH • Clear reporting and response mechanisms • Staff and participant awareness
	Accountability	• Clear documentation and reporting lines • Alignment with Global Fund requirements

2. Roles and Responsibilities	Senior Management	• Approve and endorse SOPs • Ensure alignment with GF standards • Allocate resources for safe implementation • Promote a culture of non-discrimination and accountability • Oversee accountability and incident response
	Program Management	• Integrate human rights and gender into programming • Ensure safe implementation • Monitor compliance • Coordinate with partners • Ensure incidents and violations are reported and addressed
	Safeguarding Focal Point	• Manage safeguarding reporting mechanisms • Ensure confidentiality of complaints • Coordinate survivor-centered response • Support investigations • Promote safeguarding awareness among staff
	Human Rights / Gender Focal Point	• Support gender analysis • Promote non-discriminatory practices • Advise staff on gender-responsive and rights-based approaches • Monitor stigma and barriers
	Monitoring & Evaluation Team	• Collect gender and equity-disaggregated data • Track access and equity indicators • Document incidents and program gaps • Support program review and improvement
3. Risk Assessment	Risk Identification	• Programmatic/activity-level risks • Safety and security risks (staff and participants)Legal and social risks (stigma, criminalization) • Organizational risks (data protection, HR capacity) • For activities with moderate to high complexity or risk, SRs may use the **Security Risk Assessment Matrix** (Annex 2) or an existing organizational risk assessment tool to conduct and document a structured risk assessment.
	Digital Risk Identification	• Virtual activity risks • Digital safety and confidentiality risks • Risks related to social media, chat apps, and online communication • Data protection and unauthorized information risks • Online harassment, exposure, and surveillance risks • For activities involving online engagement, SRs should assess digital safety measures and confidentiality protection before implementation
4. Operational Procedures	Safe Non-Discriminatory Service Delivery	• Equal access for key populations • Protection of confidentiality and privacy • Safe and welcoming environments • Consider conducting a participant safety briefing, where relevant and appropriate, prior to activities involving key populations (see Annex 1)
	Community Engagement	• Community-led monitoring • Peer support mechanisms • Feedback and complaint systems
	Gender-Responsive Programming	• Gender analysis • GBV referral pathways • Inclusive service delivery
	Safeguarding Procedures	• Incident reporting mechanisms • Survivor-centered response protocols • Documentation and follow-up

	Incident Reporting and Management	• Clear definition of reportable incidents (security, violence, harassment, human rights violations, SEAH) • Confidential and accessible reporting channels • Defined reporting timelines and escalation pathways • Documentation of incidents and actions taken • Survivor-centered approach (for SEAH/GBV cases) • Protection against retaliation • Linkages to referral services (legal, medical, psychosocial) • Roles and responsibilities for incident handling
5. Risk Mitigation	Mitigation Measures	• Safe outreach protocols • Secure service locations • Confidential communication channels • Emergency preparedness and response • Legal support and referral pathways • Community engagement for safe participation • Periodic review of safety measures
	Response Measures	• Immediate response and support for affected participants or staff • Safe and confidential reporting procedures • Clear referral pathways for legal, medical, psychosocial, or protection support • Defined roles and responsibilities during incident response • Communication and escalation procedures for emergencies or security incidents • Follow-up and documentation of incidents and actions taken • Measures to prevent retaliation, further harm, or confidentiality breaches
6. Community Engagement	Community Engagement and Safe Participation	• Engage KPs and trusted community representatives where safe, appropriate, and feasible • Ensure community engagement is safe, voluntary, confidential, and appropriate to the local legal, social, and security context • Involve peer educators, community focal points, KP-led organizations, or trusted community actors in the design, planning, implementation, and review of activities that affect them
	Community-Based Risk Identification and Validation	• Seek input from KPs or trusted community representatives and outreach workers before implementing activities to validate whether participation arrangements are safe, discreet, and acceptable, and to identify safety and security concerns related to activities and participation • Validate key elements such as venue selection, invitation methods, registration procedures, communication channels, transport arrangements, and confidentiality measures • Assess whether activity procedures may unintentionally expose participants, outreach workers, or community members to stigma, retaliation, or safety risks • Identify emerging community-level safety, legal, social, or operational risk that may affect participation or implementation • Adapt participation arrangements based on community concerns, contextual risks, or changing security situations

	Feedback, Complaint, and Community Review Mechanisms	• Ensure feedback and complaint mechanisms are accessible, confidential, and safe for participants and outreach workers • Encourage safe reporting of concerns, incidents, barriers, or dissatisfaction related to activities or participation • Periodically review community feedback, complaints, field observations, and incident reports to identify recurring risks or needed adjustments • Ensure feedback and review processes do not expose participants, outreach workers, or community representatives to additional risk
	Documentation and Learning	• Document community concerns, identified risks, incidents, lessons learned, and mitigation actions where appropriate • Use community feedback and lived experiences to strengthen future planning, safety measures, participation approaches, and response procedures • Consider integrating relevant findings from CRSS, KPs post-activity feedback surveys, or other feedback channels into ongoing activity improvement and risk mitigation efforts, where appropriate • Maintain confidentiality and data protection when documenting community feedback, incidents, or participation-related concerns
7. MEL	Monitoring & Reporting	• Track indicators on stigma, discrimination, and access • Document incidents and responses • Use data for program improvement
	Continuous Improvement	• Regular SOP review and updates • Adaptation to emerging risks • Alignment with legal and operational changes
8. Capacity Building	Staff Training	• Human rights and gender equality • Safeguarding and SEAH prevention • Trauma-informed approaches • Engagement with key populations

Abbreviations:

GBV gender-based violence;
HR human resources;
MEL Monitoring, Evaluation, and Learning;
SEAH sexual exploitation, abuse, and harassment;
SOP standard operating procedures.

The provision of services to all individuals without exclusion, restriction, or differential treatment based on personal characteristics such as gender, legal status, or belonging to key or vulnerable populations. Ensuring that individuals and communities are treated with respect and are empowered to participate in decisions affecting them. Activities assessed as high-risk must be reviewed and approved by senior management before implementation. Understanding gender dynamics affecting HIV risk and access.

Safety and Security Readiness Checklist

This Safety and Security Readiness Checklist is a practical and adaptable tool designed to support SRs working with key populations in assessing and strengthening organizational, operational, and activity-level safety and security considerations. The checklist is intended to support self-assessment, reflection, and continuous improvement. It may be used as presented, adapted to fit organizational contexts, or integrated into existing organizational systems, tools, or procedures. SRs may choose to use all or selected sections of the checklist depending on their operational context, identified risks, and programmatic needs. It does not replace existing organizational policies, procedures, or risk management systems. Rather, it is intended to complement and strengthen existing approaches by providing a structured set of considerations that may support planning, implementation, monitoring, and risk mitigation efforts.

This is a living resource and should be periodically reviewed and adapted to reflect emerging risks, operational realities, community feedback, and evolving safety and security considerations.

Table 2 Safety and Security Readiness Checklist

	Yes	No[a]	Action(s) Required	Responsible person	Timeline
Organizational Safety & Security					
1. Are data protection procedures in place (e.g. secure storage, restricted access)?					
2. Is personal data collected only when necessary?					
3. Are confidentiality protocols defined and implemented?					
4. Is there a safeguarding policy or mechanism in place?					
5. Is there a system for reporting risks or incidents at the organizational level?					
6. Are roles and responsibilities for safety and security clearly defined?					
7. Is sensitive information handled in accordance with internal policies?					
Human Resources & Staff Preparedness					
1. Have staff received training on working with key populations?					
2. Are staff trained on confidentiality and data protection?					
3. Is a focal point designated for safety or incident management?					
4. Are staff aware of reporting procedures for incidents?					

5. Do staff follow safe communication protocols?					
6. Are staff briefed on risks before activities?					
7. Are staff prepared to respond to safety and security concerns?					
Programmatic / Activity-Level Safety					
1. Has a safety risk assessment been conducted for this activity using the Security Risk Assessment Matrix (Annex 1), where required?					
2. Has the legal and social context been reviewed (e.g. stigma, criminalization risks)?					
3. Have risks to participants been identified (e.g. exposure of identity, harassment)?					
4. Have mitigation measures been developed (e.g. discreet communication methods)?					
5. Is the activity location safe, discreet, and accessible?					
6. Are entry and exit routes safe and discreet?					
7. Is transportation arranged safely where required?					
8. Are participants informed about the purpose of the activity?					
9. Have participants provided informed consent?					
10. Can participants withdraw from the activity at any time?					
11. Are respectful behavior and anti-harassment measures in place?					
12. Are communication methods designed to protect identities?					
13. Are invitations shared using neutral or discreet language?					

14. Are digital communication tools secure and password-protected where possible?					
15. Has a participant safety briefing been planned and included at the start of the activity (see Annex 2)?					
16. In the case of online or virtual activities, are communication channels safe and discreet?					
17. In the case of online or virtual activities, are staff or outreach workers trained on safe online communication with KPs?					
18. In the case of online or virtual activities, are personal data and digital records adequately protected?					
19. In the case of online or virtual activities, are risks related to online harassment, exposure, surveillance, or confidentiality breaches considered?					
20. In the case of online or virtual activities, is there a response plan for digital safety and confidentiality incidents?					
Emergency Preparedness & Response (Primary)					
1. Is there a clear plan for responding to security incidents?					
2. Are emergency contacts available and accessible to staff?					
3. Are first aid or medical resources available where applicable?					
4. Are participants or individuals accessing services informed of emergency procedures where relevant?					
5. Are staff trained on emergency response protocols?					
6. Is there a clear escalation and reporting mechanism for incidents?					

For each question, where applicable, specify the action(s) required, the responsible person, and the timeline, based on the nature of the question and the response provided.

Post-Activity Safety & Security Feedback Question Bank for Key Populations

This Question Bank is intended as a flexible and adaptable resource to support SRs in collecting post-activity feedback from key participants regarding safety, security, confidentiality, accessibility, participation experiences, and any concerns encountered during or following activities.

The bank of questions is designed as an adaptable and non-exhaustive resource that may be selected, modified, integrated into existing feedback or reflection mechanisms, or applied based on the nature, context, and risk level of the activity. SRs are encouraged to use a flexible, context-sensitive, and participant-centered approach when selecting and applying questions.

The purpose of this Question Bank is to support continuous learning and improvement of safety and security measures, strengthen safe participation approaches, identify potential risks or concerns, and ensure that community feedback and lived experiences inform future activities and response measures.

Feedback collection processes should be voluntary, confidential, safe, and appropriate to the local legal, social, and security context, and should not place participants or outreach workers at additional risk.

The following questions may be adapted, selected, or used based on the context and nature of the activity. Where applicable, participants may be asked to rate their level of agreement with the following statements using a scale from 1 to 5 as follows:

1 Strongly Disagree

2 Disagree

3 Neutral

4 Agree

5 Strongly Agree

NA Not Applicable

Table 3 Safety and Security Question Bank

	1	2	3	4	5	NA
Overall Safety and Risk						
1. I felt safe and comfortable participating in this activity.						
2. If any concern or issue arose (such as exposure, stigma, or harassment) it was handled in a way that made me feel safe.						
3. The overall environment (including location and surrounding context) felt safe and appropriate.						
4. I felt comfortable raising concerns or asking questions during the activity.						
5. The safety briefing at the beginning of the activity was clear and helpful.						
Confidentiality & Privacy						
1. My identity and personal information were protected through the activity.						
2. I was able to participate without sharing personal information I was not comfortable disclosing.						
3. I was clearly informed about how my information would be used and protected.						
Location & Logistics Safety						
1. The activity location was discreet and allowed me to attend without attracting unwanted attention.						
2. I felt safe when arriving at and leaving the venue.						
3. Logistics (such as transportation, entry and exit, and organization) were handled in a way that protected my safety and privacy.						
4. I felt safe after leaving the activity (e.g., traveling home, returning to my environment).						

Staff Conduct & Preparedness						
1. Staff behaved respectfully and made me feel safe and comfortable.						
2. Staff respected my privacy and handled my information appropriately						
3. I knew who to contact if I felt unsafe or needed support during the activity.						
Participant Rights & Protection						
1. I was clearly informed about the purpose of the activity and my rights as a participant.						
2. My participation was voluntary, and I felt free to withdraw at any time.						
3. I felt respected and free from discrimination, harassment, or pressure.						
4. I felt that appropriate support (e.g., legal, other services) would be available if needed.						
5. I knew what to do or who to contact in case of an emergency.						
Safeguarding & SEAH Prevention						
1. I felt safe from any form of harassment, exploitation, or abuse during the activity						
2. I was informed about how to report concerns or complaints safely and confidentially.						
Overall Assessment						
Overall, I am satisfied with the safety and security of this activity.						

Where appropriate, SRs may begin the feedback process with short confidentiality and voluntary participation statements, such as *"You are free not to answer any of the questions."* **And\Or use a disclaimer statement such as** *"Your responses are anonymous and will not be linked to your identity. You may skip any question or stop at any time. Your participation will not affect your access to services in any way. Responses will be used in aggregate to improve program safety and will not be used to identify individuals."*

The following questions may help identify additional safety concerns, participant experiences, or areas for improvement related to the activity.

Did you experience or witness anything that made you feel unsafe? (Optional)

☐ Yes ☐ No ☐ Prefer not to answer

If yes, you may describe it here (optional): ______________________________

____

Write in the box below any additional comments, concerns, or suggestions you may have. Your feedback will be treated confidentially and used to improve future activities.

Where appropriate and contextually safe, demographic questions may also be included to support understanding of participants' experiences and to inform accessibility considerations.

DEMOGRAPHIC INFORMATION (Optional)

Age Group	☐ 18-24 ☐ 25-34 ☐ 35-44 ☐ 45-54 ☐ 55+
Gender Identity	☐ Man ☐ Woman ☐ Non-binary ☐ Other ____________________ ☐ Prefer not to say
First time attending?	☐ Yes ☐ No

Annexes

Annex 1: Participant Safety Briefing Template

This template is provided as a practical reference resource that may be adapted to the context, format, risk level, and objectives of a specific activity. SRs may use this template as presented, modify it to reflect local needs and organizational procedures, or integrate its elements into existing participant briefing processes. Not all elements may be relevant to every activity, and the level of detail should be proportionate to the nature of the activity and identified risks.

Estimated Duration: 2–3 minutes

1. Welcome and Purpose

- Briefly explain the purpose of the activity.
- Clarify that participation is voluntary.
  "Welcome and thank you for being here. Today's activity is about [brief purpose]. Your participation is completely voluntary."

2. Confidentiality

- Participants are not required to disclose personal information.
  "You are not required to share any personal information unless you feel comfortable."
- Information shared during the activity should remain confidential.
  "We ask everyone to respect each other's privacy and not share what is discussed here outside this space."

3. Respectful Behavior

- Everyone must treat others with respect.
- Harassment, discrimination, or abusive language will not be tolerated.

4. Participation Rights

- Participants have the right to:
  - Ask questions
  - Decline to answer questions
  - Leave the activity at any time
- Participation or non-participation will not affect access to any services
- No one will be penalized for choosing not to participate

5. Safety and Reporting

- Participants should be informed:
  - Who is the focal point if they feel unsafe
  - How to report concerns or complaints
  - Reporting is confidential
  - That concerns will be handled confidentially
  - Reporting will not affect access to services

6. Emergency Procedures

- Participants should be informed:
  - What to do in case of an emergency
  - Who of the staff to contact for assistance
  - They can speak up at any time if something makes them uncomfortable
    "If you have any questions or concerns at any time, please feel free to speak to us. Your safety and comfort are our priority."

Closing

- "Your safety and comfort are very important to us. Please let us know if you have any questions or concerns at any time."

Annex 2: Security Risk Assessment Matrix

The Security Risk Assessment Matrix is a practical tool to support SRs in identifying, assessing, and mitigating safety and security risks associated with activities, particularly those involving heightened levels of risk. It helps assess likelihood and impact, prioritize risks, and define mitigation measures to protect participants and staff. This matrix should be adapted to the local context, local legal environment, and KP-specific vulnerabilities. It should be used alongside the Safety and Security Readiness Checklist to support informed decision-making.

When to use this tool

This matrix may be completed for activities that involve higher risk, including large gatherings, outreach with key populations, or activities conducted in sensitive legal or social environments.

The purpose of this matrix is to:
- Identify potential safety and security risks
- Assess likelihood and impact
- Develop mitigation strategies to protect participants and staff

Scoring Guidance

Risk levels are determined by assessing the likelihood of occurrence and the potential impact of each identified risk. The overall risk level is calculated as:

Risk Level = Likelihood × Impact

Scores range from 1 to 9, with higher scores indicating higher risk.

The resulting score should be used to:
- Prioritize risks
- Inform the design of appropriate mitigation measures
- Support decision-making on whether an activity can proceed

LIKELIHOOD RATING GUIDE

LOW	Unlikely to occur and minimal impact	*Score* 1
MODERATE	Possible occurrence with moderate impact	*Score* 2
HIGH	Likely to occur with serious consequences	*Score* 3

IMPACT RATING GUIDE

LOW	No or low impact	*Score* 1
MODERATE	Medium impact	*Score* 2
HIGH	High impact	*Score* 3

Risk Level Interpretation

- 1–3 = Low Risk (Proceed with standard precautions)
- 4–6 = Moderate Risk (Mitigation required before implementation)
- 7–9 = High Risk (Do not proceed without senior approval and strengthened mitigation)

Matrix

RISK CATEGORY	DESCRIPTION OF RISK	LIKELIHOOD (LOW/MED/ HIGH)	IMPACT (LOW/ MED/ HIGH)	RISK LEVEL	MITIGATION MEASURES*	RESPONSIBLE PERSON AND TIMELINE
LEGAL ENVIRONMENT	Criminalization of key populations may expose participants to arrest or harassment				Select discreet locations, avoid public exposure, and ensure confidentiality	
COMMUNITY STIGMA	Participants may face discrimination or stigma if their participation becomes known				Ensure private venues, avoid visible branding, protect participant identity	
LAW ENFORCEMENT INTERACTION	Police presence or intervention during activities				Conduct risk analysis beforehand, and establish contingency plans	
PARTICIPANT IDENTIFICATION	Participants may be identified publicly as belonging to key populations				Use confidential registration, avoid photos or public lists	
VENUE SAFETY	Location may not provide a secure or discreet environment				Select trusted venues, assess entry/exit points	
TRAVEL RISKS	Participants may face harassment while traveling to the activity				Provide safe transport guidance or reimburse travel	

STAFF SAFETY	Outreach staff may face harassment or threats during activities				Staff safety briefing and communication protocols	
DIGITAL SECURITY	Leakage of participant information through digital platforms				Use secure data systems and password protection	
ONLINE HARASSMENT OR EXPOSURE	Online harassment, exposure, or disclosure of participant or activity-related information.				Establish safe reporting and response procedures for online harassment, threats, exposure, or harmful online interactions	
GENDER-BASED VIOLENCE RISK	Participants may experience harassment or GBV linked to participation				Provide GBV referral pathways and confidential reporting	
SAFEGUARDING RISK (SEAH)	Risk of sexual exploitation or harassment during activities				Ensure safeguarding policy awareness and reporting mechanisms	
EMERGENCY SITUATIONS	Health or security emergencies during the activity				Emergency contacts and response plan available	

**The mitigation measures provided in the table are illustrative examples and should be adapted and tailored to fit your specific context and operational needs.*

Important Note: When completing the risk assessment matrix, SRs must apply a gender-sensitive and intersectionality-informed approach to the identification, analysis, and mitigation of risks. This requires recognizing that individuals may experience different levels and forms of risk based on gender and the intersection of multiple factors, including age, disability, legal status, and other contexts of vulnerability. SRs should explicitly consider risks related to gender-based violence (GBV), stigma, discrimination, and unequal power relations, particularly in activities involving key populations. All mitigation measures must be designed to address these differentiated risks and to ensure safe, inclusive, and equitable participation.

Risk Assessment Completed By:

Name: ______________________________

Position: ______________________________

Signature: ______________________________

Date: ______________________________

Reviewed/Approved By:

Name: ______________________________

Position: ______________________________

Signature: ______________________________

Date: ______________________________

The development of this Safety and Security Framework benefited from the valuable contributions, reviews, and feedback provided by our partners. We gratefully acknowledge the contributions of the Global Fund, the MENA Coalition on HIV and Human Rights (MENA-H), the Society for Inclusion and Development in Communities and Care for All (SIDC), the Association Tunisienne de Lutte contre les Maladies Sexuellement Transmissibles et le SIDA (ATL), the Forearms of Change Center to Enable Community (FOCCEC), Caritas Egypt, and the Association de Lutte Contre le Sida (ALCS). Their insights and engagement helped strengthen and refine this framework.

GHD|EMPHNET: Working Together for Better Health

The Eastern Mediterranean Public Health Network (EMPHNET) is a regional network that focuses on strengthening public health systems in the Eastern Mediterranean Region (EMR) and beyond. EMPHNET works in partnership with ministries of health, non-government organizations, international agencies, private sector, and relevant institutions from the region and the globe to promote public health and applied epidemiology. To advance the work of EMPHNET, Global Health Development (GHD) was initiated to build coordination mechanisms with partners and collaborators. Together, GHD|EMPHNET is dedicated to serving the region by supporting efforts to promote public health policies, strategic planning, sustainable financing, resource mobilization, public health programs, and other related areas.

Shmeisani, Abdallah Ben Abbas Street, Building No 42,
P.O.Box: 963709, Postal Code: 11196 Amman, Jordan

Tel: +962-6-5519962
Fax: +962-6-5519963

www.emphnet.net
info@emphnet.net