



RISK ASSESSMENT INSTRUMENT

Instructions: Please use this questionnaire as guidance in the development of your organization's Risk Mitigation and Contingency Plan. The goal of the questionnaire and plan is to give you (the Implementing Partner) and us (USAID) a better idea of your current security environment and more importantly the ability to improve and enhance that environment as a result of continuing changes in the political landscape of Uganda. Please note that including the Health Programs (Annex A) and Child Welfare (Annex B) in your Risk Mitigation and Contingency Plan is only necessary should it relate directly to your organizations' activities.

FACILITY

1. Name of office Site/Location. Please include description (residential, single office, office building, campus/compound etc.). Also include information on regional/field offices (Uganda), considering how it relates to each project/program.
2. Do you have any organization on the premises that provides security services (Head Quarters and field offices)?
 - 2a. If yes, is there external and internal security and are they the same company or different?
3. Is there guard staff?
 - 3a. If yes, are they armed or unarmed (specify any differences that exist between daytime and nighttime staff and protocol)?
4. Have you reviewed the training of guard staff?
 - 4a. How do you determine whether it is sufficient?
5. Does your security organization (or another consultant) provide risk assessment of facilities? This may include but is not limited to, bars on windows, razor wire, access to building and data, proper identification for staff and visitors, etc.
 - 5a. If yes, when was the last review and what did it include?
6. Do you have security cameras?
 - 6a. Are they in working order?
 - 6b. Was it part of your security assessment?
7. Do you have an alarm system and do you use the alarm system? Please comment for headquarters and field offices.



ACCESS

8. Do you have employee access protocols?
 - 8a. What type (e.g. codes, biometric, badges etc.)?
9. Have you developed protocols for requests by police to access your facility?
 - 9a. If so, what are they?
10. Are there certain areas of restricted access? Where? Who has access?
11. Are there procedures for allowing off-hours access?
 - 11a. If so, what are those procedures?
 - 11b. Who is aware of off-hours access?
 - 11c. Who documents off-hours access?
12. Who has access to visitor logs?
13. Do you have a plan should a group of individuals try to gain access to your facility?
 - 13a. If yes, please provide details of the plan?
14. Do you have a procedure for people showing up without appointments/unexpected visitors or without proper identification?
 - 14a. How does reception handle this?
 - 14b. If you have a campus or compound how can you track visitors and send them through one initial point of entrance?
15. Do you have or have you considered a receptionist with security background or one provided by your security organization?
16. Do you issue visitor badges or have some manner in which to distinguish between staff and visitors?

STAFF

17. Do you have a list of emergency numbers/contacts for your organization?
18. Do you have a phone tree in order to notify staff of an emergency situation?
19. Do you have a home office, 24 hour emergency number?
20. Who can employees contact on off-hours?
 - 20a. What is the protocol?
21. Does your organization/company provide office issued phones/devices?



21a. Are there

alternate ways of contacting employees?

22. Are emergency/security numbers pre-loaded into company phones?

23. What is your plan for training staff on various protocols for safety & security?

23a. How frequently is this updated?

23b. When did you last update/review these plans?

23c. Where are plans kept?

24. Does your plan address the situation of a staff member being arrested for work related to the program activities?

24a. If so, how?

25. Is employee paperwork (e.g. work permits, badges) up to date/in order?

25a. Have you received work permits for expatriate staff?

26. Do you have legal counsel?

26a. Are they capable of handling potential problems that this risk assessment attempts to address (e.g. including but not limited to effects of recent laws)?

27. If items/property is taken (either by employees, authorities, etc.) do you undertake an inventory assessment?

27a. Do you document under what circumstances are items taken?

RECORDS - (Including Personal Identifiable Information or PII)

28. What type of records do you keep that could be of interest to outside parties (often specific but not limited to health programs, also if applicable please see Health Questionnaire Annex)

29. Are records stored off-site?

29a. What type of records do they include?

29b. Are they secured and archived?

30. How do you destroy records?

31. What files (types) are kept electronically, what files are in hard copy?

32. Describe processes and details of protection of personal, programmatic and organizational data (e.g. password protection (how frequently changed), files encrypted, access to email etc.).

Regarding PII:

33. Do you plan to restrict/limit use of PII?



- 34. Have you considered replacing PII with greater anonymity (ID numbers instead of names)?
- 35. Do you have methods in place to secure confidentiality of PII?
- 36. Do you generate records that become part of the GOU records system?
 - 36a. Have you reviewed the safety/security of those records?
- 37. Is there training to make sure GOU has appropriate systems in place?
- 38. What type of records can be edited?
 - 38a. What kind of leeway do you have in restricting unnecessary information flow?

SUB-AWARDEES

- 39. How many sub-awardees does your organization manage?
- 40. Have you discussed risk assessment with your sub-awardees?
 - 40a. Do you include any type of risk assessment in a pre-award survey?
- 41. Does training for new grantees exist?
- 42. Which sub-awardees have an internal risk assessment plan?
 - 42a. Is their risk assessment plan current?
- 43. Have you reviewed the risk assessment plan?
 - 43a. What specific feedback was provided to each sub-awardee?
 - 43b. Has a revised plan been reviewed?
- 44. Does it flow down from assessment of prime but yet is still specific to sub-awardee?
- 45. What type of access to data do sub-awardees have?
 - 45a. How is it turned over to your organization?
 - 45b. Does the sub-awardee retain data?
- 46. What type of data are they collecting?
- 47. Do you keep a list of updated STTA, contact information and information of whom to contact in emergencies?

COMMUNICATIONS

- 48. Have you developed a communications strategy for implementation of a risk assessment plan with your staff?
 - 48a. With your sub-awardees?



49. Do you have a policy/protocol regarding internal communications amongst staff (conflict, differing viewpoints etc.)?
50. Do you have a policy/protocol regarding external communications (including media)?
51. If yes, who is the spokesperson(s)? Are they trained, knowledgeable to speak on controversial/politically sensitive issues?

BRANDING AND MARKING

53. Are there concerns regarding situations in which Branding and Marking policy may contribute to greater risks for you organization?
53a. If so, what are they?

COST

54. Have you calculated a cost for implementation of the risk assessment plan and possible security upgrade?
55. What types of costs do you foresee incurring?
56. Are these costs attributable to your contract/agreement?

Annex A - Supplemental Questions for Health Activities

SERVICES

1. What types of services are offered on site?
2. What services does your program refer and to whom are they referred?

Services

Referral Site

- a)
- b)
- c)
- d)
- e)

3. What are the target sub-populations?
4. How does the program work with other organizations or networks?
5. Are services provided targeted specifically for MSM or are they integrated into other comprehensive services?
6. Does the program include outreach?
7. Are there youth-specific services available?
8. Are there protocols/manuals/guides for service provision?

TRAINING

9. What HIV service providers (public, private, NGO, faith-based, etc.) have been specifically trained to provide services meeting the needs of MSM or LGBTI? Where are these facilities?
10. Is the government (Ministry of Health) a sponsor/partner in training?
11. Who provided the training?
12. What topics were covered?
13. Who attended (NGO or public health sector staff)? Peer educators?

MONITORING

14. Does the data capture LGBTI service use?



15. Are LGBTI indicators defined/disaggregated? If yes, how?
16. Please describe the data flow of the program - how is monitoring carried out (method of data collection (forms, etc.) and frequency of collection), and by whom?
17. Does this program use unique identifier or other forms of anonymous data?
18. Does the program have written data security and confidentiality policies/procedures?
19. Who has access to data?
20. Are locks keys, passwords and codes used to protect confidential information?
21. Do you have a policy related to access to data?
22. How are any breaches in confidentiality or data leaks handled (i.e. if confidentiality is broken)?
23. Do you have any contingency or emergency plan for the program in the event of threat or disappearance of records?
24. Does the program have access to legal counsel?
25. How is staff trained regarding data security?
26. When was the last training?
27. Do staff members sign a confidentiality agreement?
28. How do staff protect their computer/work station, laptop, or other devices (phones, iPads, etc.) containing confidential public health information or data?
29. When data is aggregated for reporting to external bodies, how is personal information (names, addresses, phone numbers, etc.) included?
30. In your program, is HIV status of individuals collected?
31. Is access to HIV data given for any purpose unrelated to public health (i.e. police or court order)?
32. Is access to data given to other public health organizations (i.e research)?
33. How is data stored?
34. Are patient forms, records or files taken home?
35. How do you dispose of documents with patient related data?
36. Is there an archiving policy? If so how are patient files stored and archived?
37. How is data on computers protected (password protected, encrypted, etc.)? What about paper program records?



USAID | UGANDA

FROM THE AMERICAN PEOPLE

38. Are personal identifiers removed from data sets?
39. Who has access to electronic data?
40. What are the policies/procedures regarding handling of electronic communications including e-mail or fax transmissions which may contain confidential information sent from the program? Is the electronic data being sent, encrypted?



Annex B – Supplemental Questions for Child Protection

1. Do you have any activities involved with children?
2. If yes, is there:
 - a. A child protection policy? What does it entail? How can it be strengthened?
 - b. A checklist or protocol
 - c. A code of conduct?
 - d. Background check of staff for individuals working with children? How does this take place? What records are available? What is the protocol for hiring these individuals?
 - e. Organizational capacity and input from legal counsel?