XXXX [country name]

**SECURITY PREPAREDNESS & CONTINGENCY PLAN**

**To ensure safety and security of staff, partners, communities and the organization before, during and after a trigger event**

|  |  |  |  |
| --- | --- | --- | --- |
| Developed by |  | Last reviewed on |  |
| Approved by |  | Applicable to | which area, country, region does this apply to? |

Table of Contents

[MANAGEMENT ACCOUNTABILITY 2](#_Toc63414497)

[THE CONTEXT 2](#_Toc63414498)

XXXX[’S POSITION & COMMS/MEDIA PROTOCOL 2](#_Toc63414499)

[XXXX’s SECURITY PHASES 2](#_Toc63414500)

[1.1 SCENARIO 01 3](#_Toc63414501)

[1.2 SCENARIO 02 4](#_Toc63414502)

[1.3 SCENARIO 03 5](#_Toc63414503)

# MANAGEMENT ACCOUNTABILITY

|  |  |  |
| --- | --- | --- |
| **Name and Role** | **Contact number** | **Email address** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# THE CONTEXT

* Briefly describe the trigger event for which you are developing this contingency plan.
* Give an overview of what’s happening and an outlook of what might happen in near future
* Mention key considerations, risks and opportunities, essential background.

# XXXX’s POSITION & COMMS/MEDIA PROTOCOL

* XXXX leadership should state what their position on the matter is and who will communicate with external stakeholders and media.

# XXXX’s SECURITY PHASES

|  |
| --- |
| **SECURITY PHASE 01 - NORMAL: Situation is in line with what is determined as normal. Application of SOP’s and basic precautions offer sufficient mitigation.** |
| **SECURITY PHASE 02 - POSSIBLE DETERIORATION: Situation indicates that the environment is gradually deteriorating. Some extraordinary measures may need to be applied, including the partial withdrawal of non-essential staff, visitors or accompanied legal dependents, hibernation or suspension/scale down of programmes.** |
| **SECURITY PHASE 03 – CRISIS: Situation has deteriorated to a point that presents or is likely to present immediate and serious risks to staff, consultants or visitors, or that might prohibit continuation of programmes.** |

# SCENARIO 01

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario description and Key indicators or warning signs to look for.** | **Security Phase &**  **Possibility of this happening** | **Implications for staff, programme and organisation** | **Response Strategy**   * Mention what has been done to mitigate the risk * What additional actions are planned? * By whom and by when? * Budgets? |
| What this scenario will look like?  What are the key indicators and early warning signs for you to monitor? | Refer to XXXX’s security phases   * Least likely * Likely * Most likely * Currently happening | 1. Movement and route safety? |  |
| 1. Premises and buildings (offices and official residences) – including assets and documents. |  |
| 1. Office Vehicles |  |
| 1. Supplies and access to items of daily use? |  |
| 1. Communication and internet? |  |
| 1. Reputation and perception? |  |
| 1. Programme Implementation? |  |
| 1. Staff morale and wellbeing? |  |
| 1. Direct Security threats or collateral risks for staff and partners? If not captured above.  * Physical or digital threats, crime, kidnap, attack etc. * Legal risk such as detention or arrest * Raids and inspections * Visa and work permit issues * Sexual assault * Forced removal from the pace of work or residence * Other |  |
| 1. PSEA and safeguarding risks for staff, partner and communities? |  |
| 1. Banking and cash availability? |  |
| 1. Financial budgets and sustainability? |  |
| 1. Relationship with partners, communities, government departments, social movements, and other critical stakeholders? |  |
| 1. Donor funded projects, child sponsorship activities and other internal deadlines? |  |
| 1. Risk related to internal team cohesion? |  |
| 1. Management and leadership risks? |  |
| 1. Any other organisational risks? |  |

# SCENARIO 02

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario description and Key indicators or warning signs to look for.** | **Security Phase &**  **Possibility of this happening** | **Implications for staff, programme and organisation** | **Response Strategy**   * Mention what has been done to mitigate the risk * What additional actions are planned? * By whom and by when? * Budgets? |
| What this scenario will look like?  What are the key indicators and early warning signs for you to monitor? | Refer to XXXX’s security phases   * Least likely * Likely * Most likely * Currently happening | 1. Movement and route safety? |  |
| 1. Premises and buildings (offices and official residences) – including assets and documents. |  |
| 1. Office Vehicles |  |
| 1. Supplies and access to items of daily use? |  |
| 1. Communication and internet? |  |
| 1. Reputation and perception? |  |
| 1. Programme Implementation? |  |
| 1. Staff morale and wellbeing? |  |
| 1. Direct Security threats or collateral risks for staff and partners? If not captured above.  * Physical or digital threats, crime, kidnap, attack etc. * Legal risk such as detention or arrest * Raids and inspections * Visa and work permit issues * Sexual assault * Forced removal from the pace of work or residence * Other |  |
| 1. PSEA and safeguarding risks for staff, partner and communities? |  |
| 1. Banking and cash availability? |  |
| 1. Financial budgets and sustainability? |  |
| 1. Relationship with partners, communities, government departments, social movements, and other critical stakeholders? |  |
| 1. Donor funded projects, child sponsorship activities and other internal deadlines? |  |
| 1. Risk related to internal team cohesion? |  |
| 1. Management and leadership risks? |  |
| 1. Any other organisational risks? |  |

# SCENARIO 03

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario description and Key indicators or warning signs to look for.** | **Security Phase &**  **Possibility of this happening** | **Implications for staff, programme and organisation** | **Response Strategy**   * Mention what has been done to mitigate the risk * What additional actions are planned? * By whom and by when? * Budgets? |
| What this scenario will look like?  What are the key indicators and early warning signs for you to monitor? | Refer to XXXX’s security phases   * Least likely * Likely * Most likely * Currently happening | 1. Movement and route safety? |  |
| 1. Premises and buildings (offices and official residences) – including assets and documents. |  |
| 1. Office Vehicles |  |
| 1. Supplies and access to items of daily use? |  |
| 1. Communication and internet? |  |
| 1. Reputation and perception? |  |
| 1. Programme Implementation? |  |
| 1. Staff morale and wellbeing? |  |
| 1. Direct Security threats or collateral risks for staff and partners? If not captured above.  * Physical or digital threats, crime, kidnap, attack etc. * Legal risk such as detention or arrest * Raids and inspections * Visa and work permit issues * Sexual assault * Forced removal from the pace of work or residence * Other |  |
| 1. PSEA and safeguarding risks for staff, partner and communities? |  |
| 1. Banking and cash availability? |  |
| 1. Financial budgets and sustainability? |  |
| 1. Relationship with partners, communities, government departments, social movements, and other critical stakeholders? |  |
| 1. Donor funded projects, child sponsorship activities and other internal deadlines? |  |
| 1. Risk related to internal team cohesion? |  |
| 1. Management and leadership risks? |  |
| 1. Any other organisational risks? |  |

**Staff Advisory Template**

**Background & Intro**

* What is happening, few lines
* What it means for XXXX staff, allies, partners, programmes and communities – few lines
* The purpose of this communication

**XXXX Safety and Security Systems:** (please no details or political analysis, just crisp bullet points)

* Mention staff check in system
* Mention incident reporting and response system. Mention who’s on duty throughput the period and who should be reached in case of a problem, or if security/safety support is needed.
* Programmes continuing or on hold? Mention it?
* Official travel and office status, provide the latest
* What about office vehicles?
* XXXX Media policy – who will speak to the media, where should the media request be sent to?
* How are you supporting partners, allies, etc.? What mechanism is in place for getting info from the partners and communities?
* What contingency plans are in place in case if comms breakdown or internet/mobile disruption.
* Anything else?

**Staff Advisory: (**in this section provide very clear actions, do’s and don’ts for staff, keep it simple and to the point.)

Do’s:

* Stay abreast of the situation by following media etc. (add more)
* Stock up essential items in reasonable quantities including medicines, appropriate amounts of emergency cash, food, etc.
* Fuel, back up internet etc.
* Limit movement to hotspots (provide hotspot names if available)
* Respond to check-in and head count calls. (remind when and how this will be done). Let your line manager know of your whereabouts if you plan to travel.
* Report concerns and incidents promptly to xxxxx
* Participate in the democratic process as citizens but steer clear of provocation, confrontation etc. when you feel it may cause safety/security concerns (unless you are prepared to deal with the consequences).
* Reinforce residential safety
* Abide by any official rules and regulations imposed by the authorities such as curfews, movement restriction etc.
* Follow health and safety measures to reduce the risk of COVID-19 infection.
* What else?

Don’t’s:

* Don’t speak to the media or post political messages on social media unless you have been authorized to do so by XXXX
* Don’t venture out unnecessarily unless you are aware of the situation and prepared for the consequences.
* Don’t visit the hotspots without good reason
* What else?