

## SECURITY PERSONNEL MANAGEMENT PLAN

### I. Objective

The securing of the site to protect it from intrusion exposes the local communities to the abusive use of force by the site security personnel. Therefore, it is necessary that the system deployed to secure the site complies with the present security management plan.

### II. General Conditions

#### A. Scope of Application

Applicable to security sub-contractor

#### B. Applicable regulation

IFC (2017), *Good practice handbook, Use of security forces: assessing and managing risks and impacts*.

### III. Measures

#### Risk assessment

IFC identifies three levels of exposition to security risks for a project.

Potential Risks to a Project That May Require a Security Response		
More Common Risks	More Serious Risks	Rare, Severe Risks
Most projects have at least some risk of these occurring	Projects in more complex security environments may face these risks	Few projects face such intense security risks, which typically are found only in more conflicted areas
Trespassing	Robbery	Invasion/occupation of company land or property
Vandalism	Assault	Riot
Petty theft	Armed protest	Hostage taking
Roadblock	Sabotage of company property or operations	Kidnapping
Community protests	Shooting or other use of offensive weapons	Personal or communal attacks causing fatalities (e.g., bombing, murder, etc.)

IFC (2017). *Good practice handbook, Use of security forces: assessing and managing risks and impacts*.

## **Background checks and hiring**

ARISE Ivoire HSE team:

- Conduct a preliminary background check on the company or security personnel recruited to ensure that they were not involved into previous allegations of human rights violations, excessive force use or disproportionate security response.
- The background check will rest on interviews and credentials checking with past employers and will allow avoiding selecting companies or individuals with history of past abuse. The background check must be documented in written.

## **Code of conduct**

ARISE Ivoire HSE team:

- Request each security worker to sign a Code of conduct which underline its obligations, the respect due to local communities and the conditions in which they will be exposed to sanctions.
- The code of conduct is based on the general workers 'code of conduct with an additional section targeting the security personnel as follow:
- "As a security personnel, I hereby commit to comply with the following requirements:
  - To adopt at all time a benevolent, calm and peaceful behaviour and not to engage into aggressive or menacing attitudes towards the site personnel, the local communities or any intruder or person threatening the site integrity.
  - To accomplish my missions of securing the site perimeter at all times with the means at my disposal without bringing in other means that are not part of my equipment (sticks, machetes).
  - To respect the chain of command and declare all incidents according to the instructions that were communicated to me.
  - Never to use force in any form unless my life is directly threatened as per instructions that were communicated to me.
  - To arrest site intruders and to let them go with a warning in case no harm was done on site.
  - To report intruders to the gendarmerie in case of flagrant theft or degradation.
  - To welcome local community members who want to raise a claim to the project and to orientate them to the claim management mechanism of ARISE Ivoire.
  - In case of infraction to this code of conduct, to be exposed to first warning followed by dismissal for serious misconduct in case of recurrence of the infraction to this code of conduct."

## **Security responses**

The tables below present the potential responses to be adopted by security personnel and the responses that are strictly prohibited.

### **Allowed security responses**

<b>Passive deterrents</b>
---------------------------

Access Control	Physical measures to prevent access to or passage through restricted areas, such as gates, signage, guards, fences, surveillance systems, etc.
Visual presence of security	Guards (and guard dogs) stationed at access points to process ingress and egress, but who also serve as a visible deterrent
Observe and report	Guards observe, report, and record activity.
<b>Active deterrents</b>	
Verbal instructions, warning, refusal of passage/entry	Guards issue verbal warnings to people who attempt or threaten to attempt to circumvent physical security measures. The warnings may include notice that additional security is being called.
Show of force	Guards increase their numbers or demonstrate their weapons as visual indications of potential escalation of security response.
Reasonable detention	Guards detain people discovered to have trespassed or committed theft, etc., on the company site for only as long as it takes for police to arrive and assume responsibility.
<b>Escalation</b>	
Use of nonlethal force	Guards use nonlethal force defensively (e.g., batons, nonlethal ammunition) to repel an external physical threat, subject to existing use-of-force protocols.
Arrest by public authorities	Guards request the intervention of police to apprehend and/or arrest people alleged to have committed criminal acts such as theft, trespass, assault.
Lethal force (to protect life)	Guards use lethal force defensively to protect against an immediate threat to human life, subject to existing use-of-force protocols.

IFC (2017). *Good practice handbook, Use of security forces: assessing and managing risks and impacts.*

#### Prohibited security responses

Security response	Description
Intimidation or harassment	Guards use their position (or, in particular, their weapons or guard dogs) as a tool for intimidating or harassing community members, especially where no immediate risk or threat is present
Inappropriate detention	Guards detain people either for no legitimate reason, or for longer or in conditions other than what is acceptable.
Inappropriate use of force	Guards use nonlethal force offensively, or outside of acceptable use-of-force protocols, or for illegitimate reasons (such as for purposes of criminal activity, etc.).
Assault or torture	Guards detain people and physically or psychologically harm a detainee

Inappropriate use of lethal force	Guards use lethal force offensively, or outside of acceptable use-of-force protocols, or for illegitimate reasons.
-----------------------------------	--

IFC (2017). *Good practice handbook, Use of security forces: assessing and managing risks and impacts.*

### **Use of force protocol**

A use of force protocol is set up, which describes the situations where the use of force both non-lethal and lethal is prohibited.

Based on this protocol, the use of force covers any action that might bring physical harm to a third-party including: hits on the head of body, twisting of body members, tying hands or other body parts, pushing to make fall, strangling, stabbing, etc.

The use of force must always be prohibited unless the security personnel's life or another person's life is directly threatened by a third-party. A life-threatening situation is described as a situation where the life of a person is at immediate risk because the assailant is equipped with one or several sharp objects, firearms or any military devices that might cause injuries or death.

The protocol is clearly communicated to the guards so that they know how to behave in each situation.

### **Training**

ARISE Ivoire HSE Team trains the security personnel on his role and responsibilities upon recruitment and on a regular basis afterwards. Training should focus on the following topics:

- **Missions of the personnel:** securing the site with the means at their disposal, relying on a defined chain of command in case of incidents.
- **Typical security responses** to have in the face of various situations, as set up in the use-of-force protocol.
- **Appropriate behaviour** covering the physical attitude, verbal language that the personnel must adopt at all times. Both should be benevolent, calm and peaceful and devoided of any aggressive tone or menacing gestures.
- **Role in community relations:** explain that the personnel is exposed to community interactions and as such, must accept these interactions and try to assist local individuals whenever they have a query and inform them about the existence of a grievance mechanism where communities can lodge their claim.
- **Use of force:** the use of force protocol must be followed at all times, and force is allowed only in life-threatening situations and prohibited in all other situation.
- **Sexual harassment:** remind the personnel that engaging into sexual harassment against women from the local communities is prohibited and will lead to sanctions as per the Code of conduct.
- **Chain of command.**

### **Recourse to public police forces**

The cases where recourse to public police forces and the army will be required for support are as follows:

- In case of intrusion on site without theft, the intruder will be escorted out of the site premises with a warning not to reiterate the intrusion.

- In case of intrusion on site and theft, degradation of material, the gendarmerie is called upon to perform an inquiry.
- In case of civil unrest targeting the site (large-scale protests, blockades of site entrances, use of firearms or explosive devices against the site), the army must be called in.

The decision to call on the public police forces rests in the Arise Ivoire HSE team.

### **Daily report and chain of command**

The security personnel must make a daily oral or written report on its activities to the HSE supervisor.

In case of intrusion on the site or any other threat, the personnel will contact immediately the HSE supervisor to decide on the actions to be taken (no action, call on the gendarmerie, etc.).

The guardhouse will be equipped with a list of contact number and a scheme presenting the chain of command.

<b>Monitoring indicators</b>	<ul style="list-style-type: none"> <li>• number of codes of conduct signed,</li> <li>• number of security personnel trained,</li> <li>• number of incidents reported by security personnel,</li> <li>• number of complaints lodged in relation to security personnel behaviour</li> </ul>
<b>Reference documents</b>	Grievance mechanism
<b>Procedure approved by</b>	
<b>Emission/last revision date</b>	