# Annex B. Guidance for Drafting a Security Management Plan

*There are many ways to structure a Security Management Plan. The topics below are commonly included in comprehensive Security Management Plans. These can be used by companies developing their own security plans in-house, or by companies evaluating the security plans delivered by external consultants.*

*Text in black is sample text to use or modify. Text in blue italics is guidance to be considered and then replaced or removed.*

## A. Objectives, Mission, and Approach

### 1. Objectives of a Security Management Plan

* The plan is designed to guide the company’s actions at the project in protecting against and mitigating risks of a security (as well as a human rights) nature that could threaten communities, employees, facilities, and ability to operate, as well as the reputation of the company and its global operations.
* The plan provides direction, organization, integration, and continuity to the security and asset-protection program. It is written with the understanding that effective security and regard for human rights are compatible.
* The systems outlined in the plan will be maintained throughout the lifetime of the project.
* The plan will be reviewed on an *annual* basis and after any change in the security-related context in which the project operates.

### 2. Mission of Company Security

* The mission of company security is to ensure that all staff, contractors, and visitors working at the project site and in the project area are able to do so in a safe and secure environment. It also ensures that all facilities are kept safe and secure, and that all project operations are unhindered. It provides effective security-operational support to all project activities.
* Project security will approach its mission with the understanding that good security and respect for the human rights of employees and communities are fully compatible, as reflected in security forces’ behavior, communication, use of force, etc.
* *If applicable, describe the relationship between and relative responsibilities of project security and other third-party contractors and affiliated companies, such as Engineering, Procurement, and Construction (EPC) contractors.*

### 3. Approach of Project Security

*Discuss the project’s overall integrated approach for security. For example:*

* Many security risks flow out of both inherent local social issues, such as ethnic tensions, and unrecognized issues between the project and local communities. As such, project Operations, Government Relations, and Community Relations staff are all involved in the security process.
* Key stakeholders from local communities are also included in assessing security risks and in considering how to mitigate and manage those risks. Security arrangements are transparent, to the extent possible and appropriate, and are included in disclosure to and consultation with the local communities.
* The project’s grievance mechanism is an important tool for reducing potential security risks.

## B. Policies and Standards

### 1. References to Company Policies and Documents

The following company policies and documents guide security management:

* Project Security Risk Assessment
* Corporate Security Policy
* Ethics *[and/or Human Rights]* Policy
* Use of Force Policy

### 2. Other Relevant Laws and Standards

The company adheres to the following guidelines, standards, and laws:

* National laws
* Applicable international laws
* IFC Performance Standards
* Voluntary Principles on Security and Human Rights
* UN Code of Conduct for Law Enforcement Officials
* Basic Principles on the Use of Force and Firearms by Law Enforcement Officials

## C. Overview of Security Situation

### 1. Project Setting

*Provide a general description of the national and project-area security environment. This would include descriptions of:*

* *Relevant demographic information, such as population age breakdown, unemployment, poverty, and inequality;*
* *Crime levels and type;*
* *Endemic political, social, or labor unrest;*
* *Terrorism or insurgency; and*
* *General attitude toward the project and associated issues.*

### 2. Security Risks

*(Attach security risk matrix and Security Risk Assessment as annexes.)*

*This section should be based on the project Security Risk Assessment and should discuss:*

**Internal Risks**

* *These are caused by the illegal, unethical, or inappropriate behavior of project personnel or those directly affiliated with it.*
* *Most common risks would be employee theft, workplace violence, and labor unrest, potentially with associated sabotage.*
* *A security response might result in risks to employees or other individuals.*

**External Risks**

* *These are caused by the actions of people outside the project who seek to take advantage of opportunities presented by the development and operation of the project.*
* *These may include common criminal activity; disruption of the project for economic, political, or social objectives; and other deliberate actions that have a negative impact on the effective, efficient, and safe operation of the project. In extreme cases, these could include terrorism, armed insurgency, coups, or war.*
* *A security response might result in risks to communities or individuals.*
* *The presence of security forces might pose additional risks to communities or individuals.*

### 3. Security Arrangements

**Private Security**

* *Describe who provides basic project-site protection, such as the project private security force (in-house or contracted).*

**Public Security**

* *Describe briefly the local public security forces that would be called on to assist the project. This would briefly outline location, capabilities, mission, and relation to the project.*

## D. Physical Security

*Provide an overall description of the project security approach and systems. More detailed design information (such as exact CCTV camera positioning) belongs in an annex. Ideally this section includes a description of the project’s:*

* **Security Barriers—***such as fences, gates, locks, fortifying facilities, and means of access control.*
* **Surveillance/Electronic Security Systems—***including CCTV, Intrusion Detection Systems, and surveillance guard posts and patrols.*
* **Security Control Center—***describing* *the means for bringing together reporting and controlling response.*

## E. Security Operating Procedures

*Provide a brief description of key security operating procedures. Detailed standards and procedures that provide a transparent and accurate process for managing security functions (such as checklists) should be contained in an annex. Key procedures should include a brief description of the following (as appropriate) and how they fit together:*

* **Boundary Security—***how security will maintain control of the project’s perimeter and channel people to access-control points.*
* **Access-Point Operations—***the types of checks and screening for both people and vehicles at gates or other access points. Include entry and exit searches and purpose, and who is subject to it. Outline key ground rules, such as:*
	+ Searches will only be conducted by security personnel who have received instruction and information regarding the procedure and the legal aspects of search and seizure;
	+ Body searches will only be conducted by security personnel of the same gender.
	+ **Incident** **Response—***how security will respond to an incident and who is responsible for responding. Responses should be based on proper and proportional use of force. Describe the role of public security, including when they are called and by whom.*
	+ **Security Patrols—***what patrols check and how often.*
	+ **Travel Security—***(if applicable) any special procedure for offsite travel security.*
	+ **Materials Storage and Control—***(if applicable) any controls over the transport, inventory, and maintenance of any commercial explosives or chemicals (e.g., cyanide) necessary for the project. Note that these are stored in accordance with appropriate national laws and regulations.*
	+ **Information and Communication—***procedures for categorizing, handling, and controlling sensitive information.*
	+ **Firearms Security—***project policy regarding firearms onsite, as well as the responsibilities and procedures for issuing and storing any security firearms, ammunition, and less lethal weapons. This should include:*
* *Location for storage,*
* *How weapons are secured during storage,*
* *Records for issuance,*
* *Who they may be issued to,*
* *Safeguarding while in possession of the guard, and*
* *Audits.*

*Include in an annex detailed standards and procedure for weapons issuance, storage, and audit.*

## F. Security Supervision and Control

### 1. Management Structure and Responsibility

* *Explain the overall lines of control, accountability, and supervision for the security effort.*
* *Define who supervises daily performance of the security-guard force and who has authority.*
* *Describe who has overall responsibility for security information sharing and communication.*

### 2. Responsibility for Conducting Security Risk Assessments

* *Discuss the responsibilities for conducting risk assessments, who participates in them (e.g., senior management, Community Relations team, key stakeholders from communities, etc.), and what the assessments cover.*

### 3. Cross-Functional Coordination

* *Describe interdepartmental coordination.* Community Relations, Human Resources, and Government Relations are important partners in project security.
* *Outline any planning/coordination activities between security and other departments, which may range from participation in security risk assessments to weekly meetings.*

## G. Private Security Force Management

### 1. Security-Guard Force Role

* Private security’s role is to provide preventive and defensive services, protecting company employees, facilities, equipment, and operations wherever they are located.
* Private security personnel have no law-enforcement authority and will not encroach on the duties, responsibilities, and prerogatives reserved for public security forces.

### 2. Provision and Composition of the Security-Guard Force

*Describe whether members of the guard force are direct employees or from a third-party security provider.*

In developing its guard force, the project *(or its third-party provider)* will:

* Hire in accordance with national labor laws,
* Give preference in hiring to qualified local candidates where possible, and
* Promote diverse hiring practices, including gender and indigenous inclusiveness.

**Security Contractor Management** (if applicable)

* The project assumes responsibility for the oversight of security.
* *Describe how the project will actively set the standards for and oversee private security contractor selection and performance.*
* **Selection—**In selecting a security provider, the project will perform proper due diligence that will include screening for institutional reputation, training standards, procedures for screening employees, and any history of allegations of human rights abuses or other criminal behavior.
* **Contract provisions—***Include any provisions (e.g., for uniforms and equipment).*
* **Active oversight of contractor performance—**To ensure proper performance, the project will undertake audits, assist with training, inquire into any credible allegations of abuse or wrongdoing, and monitor site performance on an ongoing basis.

### 3. Security Guard Background Screening

* The project *will perform and/or require its security provider to perform* valid background checks on potential employees to screen for any allegations of past abuses, inappropriate use of force, or other criminal activity and wrongdoing.
* No guard or employee on whom there is credible negative information on these checks will serve on the project.
* These checks will be documented and maintained in individual personnel records, which are subject to review by the project.

### 4. Security-Guard Force Equipment

* *Describe equipment to be provided to guards, including radios, non-lethal weapons, and any firearms and ammunition. Guards should only be armed if it is justified by the Security Risk Assessment and is the only viable and effective mitigation measure for a clear threat.*

### 5. Security Guard Use of Force

* The use of force by private security is only sanctioned when it is for preventive and defensive purposes in proportion to the nature and extent of the threat.
* When it is necessary to arm the guard force, the project will ensure that those who are armed exhibit high levels of technical and professional proficiency and clearly understand the rules for the use of force. This means being properly trained on using force effectively, proportionally, and with respect for human rights.

### 6. Security-Guard Force Training

* The project commits to maintaining the highest standards of guard-force technical and professional proficiency through a comprehensive training program. *Outline the training responsibilities of either the security provider or the company, as applicable.* The project will review any third-party security provider’s training program and, where necessary, augment the training through the use of qualified third parties or direct instruction.
* The project will ensure that security personnel receive procedural or knowledge training in:
* Basic guarding skills,
* Guard-post orders and procedures,
* Proper conduct and ethics/human rights,
* Rules of engagement,
* Rules for the use of force,
* Adequate weapons training (as applicable), and
* Health, Safety, and Environment (HSE) mandatory training.
* *Outline how training completion records will be kept.* Training will be open to inspection/audit.

## H. Managing Relations with Public Security

### 1. Public Security Force Role

* Public security forces have responsibility for responding to and investigating all criminal activity. They also have the primary responsibility for controlling demonstrations or civil disorder. For incidents involving criminal violations or potentially violent confrontations or demonstrations, they are requested to respond to protect company personnel and property.

### 2. Engagement with Public Security Forces

* *Describe how the project will maintain constructive relations with public security (typically the police and, under certain circumstances, the military) operating in the project area or responsible for assisting project security. The depth of this section will vary with the security arrangements involving local public security forces.*
* *If it is only normal law-enforcement activities, such as investigating reported crimes or responding to an incident, ongoing engagement or liaison activity may be sufficient.*
* *If public security forces are actually assigned to the project to provide some aspects of security, then this section should describe provision of any equipment or other support, the role of the public security force, joint contingency planning, and coordination mechanisms.*
* *It should also discuss the establishment of any memorandum of understanding necessary to make the arrangements transparent.*

## I. Incident Reporting and Inquiry

* *Outline the grievance mechanism, reporting requirements and structure, and inquiry protocols about security incidents, use-of-force incidents, and allegations of abuse, misconduct, or other wrongdoing by security personnel.*
* *Discuss the responsibilities and timelines for conducting inquiries on allegations and incidents, including:*
* The company makes a commitment to expeditious inquiry into any allegations of abuse or wrongdoing.
* The private security contractor may conduct its own inquiry of an incident or allegation, but the project can conduct an independent inquiry on any serious abuse allegation or use-of-force incident.
* The inquiry findings will include a recommendation of any appropriate disciplinary action and policy or procedure changes that may be needed.

## J. Community Engagement

* *Describe how the company will engage with communities on matters relating to security. This may be done in coordination with the Community Relations department, depending on the project.*
* The project acknowledges that it may have an impact on communities and strives to mitigate risks. It will do this by providing:
* Regulations for guard offsite behavior,
* Protocol for arrangements with public security,
* Shared information on security arrangements (as appropriate), and
* Grievance mechanism for community members to report issues.