IFC’s Good Practice Handbook available online at www.ifc.org/securityforces
IFC’s Security Forces Handbook

- Practical, project-level guidance
- For private sector – IFC clients & other companies/consultants
- Focused on PS4 implementation
- Downloadable tools
IFC Performance Standards

PS1: Assessment and Management of E&S Risks and Impacts

PS2: Labor and Working Conditions

PS3: Resource Efficiency and Pollution Prevention

PS4: Community Health, Safety and Security

PS5: Land Acquisition and Involuntary Resettlement

PS6: Biodiversity Conservation and Sustainable Management of Living Natural Resources

PS7: Indigenous Peoples

PS8: Cultural Heritage
Overview

Community Health and Safety

Emergency Preparedness

Security Personnel

para 1-4

para 5-10

para 11

para 12-14

Box 1: IFC Performance Standard 4—Security

Security Personnel

12. When the client retains direct or contracted workers to provide security to safeguard its personnel and property, it will assess risks posed by its security arrangements to those within and outside the project site. In making such arrangements, the client will be guided by the principles of proportionality and good international practice in relation to hiring, rules of conduct, training, equipping, and monitoring of such workers, and by applicable law. The client will make reasonable inquiries to ensure that those providing security are not implicated in past abuses, will train them adequately in the use of force (and where applicable, firearms), and appropriate conduct toward workers and Affected Communities; and require them to act within the applicable law. The client will not sanction any use of force except when used for preventive and defensive purposes in proportion to the nature and extent of the threat. The client will provide a grievance mechanism for Affected Communities to express concerns about the security arrangements and acts of security personnel.

13. The client will assess and document risks arising from the project’s use of government security personnel deployed to provide security services. The client will seek to ensure that security personnel will act in a manner consistent with paragraph 12 above, and encourage the relevant public authorities to disclose the security arrangements for the client’s facilities to the public subject to overriding security concerns.

14. The client will consider and, where appropriate, investigate all allegations of unlawful or inappropriate acts by security personnel, take action (or urge appropriate parties to take action) to prevent recurrence, and report unlawful and abusive acts to public authorities.

PS4: Community Health, Safety and Security
• **PS4 Para 12: Private Security**
  - Risk assessment
  - Hiring and employment
  - Conduct & use of force
  - Training
  - Grievance mechanism

• **PS4 Para 13: Public Security**
  - Risk assessment
  - Seek to ensure appropriate actions

• **PS4 Para 14: Allegations & incidents**
  - Assess & address
PS4 Requirements in the Handbook

• **PS4 Para 12: Private Security**
  - Chapter 2 (risk assessment)
  - Chapter 3 (managing private security)
  - Chapter 5 (security management plan)

• **PS4 Para 13: Public Security**
  - Chapter 2 (risk assessment)
  - Chapter 4 (managing relationship w/public security)

• **PS4 Para 14: Allegations & Incidents**
  - Chapter 6 (assessing allegations/incidents)
PS4 REQUIREMENTS – QUICK REFERENCE

1. Assess Risks
   Assessing security risks can be simple and straightforward in low-risk contexts. The person responsible for security—ideally with input from other departments—should consider:
   - Security Risks (p. 23)
     What might reasonably happen that would require some type of action by security (security guards, police, army)?
   - Security Response (p. 24–25)
     How are those security personnel likely to react and respond to those identified risks?
   - Potential Impacts (pp. 26–29)
     What are the potential impacts from that response, focusing especially on impacts on communities?

2. Prevent and Mitigate Impacts
   As with other Performance Standards issues, companies should seek to avoid, minimize, and compensate for or offset negative impacts. Where potential risks or impacts are identified, companies should consider two key questions:
   - How can potential risks or impacts be prevented before they happen?
   - How can negative impacts be mitigated after they happen?
   Companies can prevent or mitigate negative impacts through corporate policies and engagement with private security (Chapter III) or public security (Chapter IV). These efforts should also be reflected in a Security Management Plan (Chapter V, pp. 81–87). In low-risk contexts, this plan may be relatively brief and may be incorporated into other policies and procedures as part of a company’s broader Environmental and Social Management System.

3. Manage Private Security
   Private security guards may be company employees or be contracted through a third-party security provider. Regardless, companies retain responsibility for ensuring that minimum standards are met—either through their own contracts and enforcement or through oversight of private security providers. This includes attention to:
   - Verifying (pp. 46–47)
     Is the provider providing security? Does anything in the guards’ background give cause for concern? Companies need to make reasonable inquiries to ensure that no guard has a history of past abuse or dishonesty. This may involve background checks or cross-checking with other companies, domestic or foreign government officials, UN missions, etc., as appropriate to the country context.
   - Ensuring appropriate use of force (pp. 46, 48)
     Do guards know what is expected of them? Are they prepared to react with appropriate and proportional force in any situation? Companies should use their policies and procedures, reinforced by training, to provide clear instructions to directly employed guards. This can be as simple as including a clause in the employment contract setting out expectations, and following up with training.
   - Training (p. 49)
     What will a guard do if a community member approaches in a non-threatening way? In a threatening way? Training should focus on appropriate behavior and use of force. In low-risk contexts this can involve just a brief review of policies and procedures, recorded in a log, to ensure that guards understand how to respond to common interactions and scenarios.
   - Equipping (pp. 49, 51)
     Do guards have what they need to do their jobs properly and safely? This usually means a uniform and identification and some type of communication device (typically a radio). In some cases it includes non-lethal weapons, such as pepper spray. The decision to arm guards with lethal force, such as a gun (pp. 51–52), is a serious one that should derive from the assessment of risk and be accompanied with a dedicated training program.
   - Monitoring (p. 53)
     Are guards performing professionally and appropriately? Companies should check to confirm that policies and procedures remain relevant, and that guards are aware of and following them.

4. Manage the Relationship with Public Security
   Particularly in low-risk contexts, companies may have limited interactions with public security forces—this is especially true regarding national forces, such as the army or navy. Still, most companies are likely to need support from at least the local police in the case of an incident, and it’s important to understand who will be responding, and how. The focus is on assessment and engagement, building on key questions, such as:
   - Public Security Response (pp. 62–65)
     What are public security forces likely to be involved in? (E.g., only when called on, or potentially in other cases as well?) What type of individual or unit is likely to respond? How are they likely to respond? (E.g., what kind of capacity, mandate, reputation, etc., do they have, and how might this apply to likely scenarios involving the company?)
   - Engagement (pp. 65–76)
     Are there opportunities to establish a relationship with police or other relevant public security forces? Companies are encouraged to reach out to authorities—preferably in advance of any issue—to understand potential deployments and, to the extent possible, to promote appropriate and proportional use of force. In low-risk contexts, this may involve simply making introductions to the local police commander and initiating a discussion about when and how authorities are likely to respond to incidents at the company or involving company personnel.
   - Documentation (p. 75)
     Companies should document their engagement efforts, whether or not they are successful (e.g., in a basic meeting log with dates, attendees, and key topics).

5. Address Grievances
   When security problems arise or communities have complaints, companies should ensure that they have a method to respond. This generally involves:
   - Receiving Complaints (p. 94)
     How can communities share information about allegations or incidents? (What is the company’s grievance mechanism?) How are complaints recorded and information collected?
   - Assessing (p. 95)
     How are complaints considered? What type of inquiry is undertaken for more serious issues? (What is the company’s inquiry procedure?) Companies should record their information, analysis, and any conclusions or recommendations in a basic memo or incident report.
   - Reporting (p. 95)
     Alleged illegal acts should be reported to the proper authorities.
   - Acting and Monitoring (pp. 95–96)
     What can be done to prevent recurrence? Are remedial actions needed for affected parties? Companies are encouraged to identify lessons learned and to integrate these into future practices and, where appropriate, to communicate them to external stakeholders.
Chapter 2: Risk Assessment

- Assess security risks to
- Identify, evaluate, and prioritize risks and likely security responses
- Understand and respond to community concerns and perceptions
- Determine appropriate security arrangements
- Inform mitigation plans and project resource implications
10 Questions All Companies Should Answer

1. What are the potential risks to the project that may require a security response?
2. How likely is it that these risks will occur?
3. What would be the likely security response?
4. If a security incident/response happens, what would be the impacts on the company?
5. How severe would these impacts be on the company?
6. If a security incident/response happens, what would be the impact on the community?
7. How severe would these impacts be on the community?
8. What are possible mitigation measures that prevent or reduce negative impacts?
9. Which risks are highest priority for mitigation, based on likelihood and severity of impact?
10. Is a full Security Risk Assessment needed?
# Security Risk Assessment

## Potential Risks to a Project That May Require a Security Response

<table>
<thead>
<tr>
<th>More Common Risks</th>
<th>More Serious Risks</th>
<th>Rare, Severe Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most projects have at least some risk of these occurring</td>
<td>Projects in more complex security environments may face these risks</td>
<td>Few projects face such intense security risks, which typically are found only in more conflicted areas</td>
</tr>
<tr>
<td>Trespassing</td>
<td>Robbery</td>
<td>Invasion/occurrence</td>
</tr>
<tr>
<td>Vandalism</td>
<td>Assault</td>
<td></td>
</tr>
<tr>
<td>Petty theft</td>
<td>Armed protest</td>
<td></td>
</tr>
<tr>
<td>Roadblock</td>
<td>Sabotage of company property or operations</td>
<td></td>
</tr>
<tr>
<td>Community protests</td>
<td>Shooting or other use of offensive weapons</td>
<td></td>
</tr>
</tbody>
</table>

## Potential Responses by Security Personnel

### Passive Deterrents
- Access Control
- Physical measures to prevent access to or passage through restricted areas, such as gates, fences, or barriers.

### Active Deterrents (*Actions that are never acceptable are in purple italics*)
- 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 be specific (e.g., “This area is restricted to authorized personnel only.”) or general (e.g., “You are trespassing.”) depending on the circumstances.

### Escalation (*Actions that are never acceptable are in purple italics*)
- 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.
## Sample SRA & Heat Map

<table>
<thead>
<tr>
<th>STEPS</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk</td>
<td>Likelihood</td>
<td>Security Response</td>
<td>Impact on Company</td>
<td>Severity</td>
<td>Impact on Community</td>
<td>Severity</td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td><strong>[Risk 1]</strong> Theft</td>
<td>4</td>
<td>Access controls to prevent theft; private security guards may apprehend suspected thieves and turn them over to authorities</td>
<td>Loss of company property; potential danger to employees if thieves take property by force</td>
<td>2</td>
<td>Alleged thieves risk injury or mistreatment during apprehension and/or detention</td>
<td>3</td>
<td>Ensure that guards have clear guidelines for apprehension and short-term detention; encourage police to treat suspects appropriately</td>
<td></td>
</tr>
<tr>
<td><strong>[Risk 2]</strong> Protest</td>
<td>3</td>
<td>Prevent or control access to site; public security may respond physically if protest becomes violent</td>
<td>Disruption to operations, particularly staff access to site and transportation; possible injury to employees</td>
<td>4</td>
<td>Injuries sustained from any use of force (justified or otherwise) against a protest; community resentment toward company</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>[Risk 3]</strong> Trespass</td>
<td>2</td>
<td>Access controls to prevent access, including clear signage; guards may confront people attempting to walk through site</td>
<td>Potential safety hazard and disruption to operations</td>
<td>2</td>
<td>Frustration among community that pre-existing access/transit routes are no longer available; injuries sustained by community members entering hazardous areas of the site</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>[Risk 4]</strong> Harassment of women by security guards</td>
<td>3</td>
<td>Presence of security forces generates potential threat</td>
<td>Limited immediate impact; potential secondary impact to operations and/or reputation from community reaction</td>
<td>1</td>
<td>Verbal harassment and/or physical violation of community members, particularly women</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Private Security

Private security → within company’s control

### Areas to Consider:

<table>
<thead>
<tr>
<th>Oversight</th>
<th>Contract</th>
<th>Vetting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retain control over and responsibility for employees’ behavior and quality</td>
<td>Include performance standards and monitoring provisions</td>
<td>Check backgrounds and avoid hiring anyone with history of abuse</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conduct</th>
<th>Use of Force</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require appropriate behavior through policies and procedures, reinforced through training</td>
<td>Ensure force is used only for preventive and defensive purposes and in proportion to the threat</td>
<td>Train guards on use of force, appropriate conduct, and firearms</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Equipping</th>
<th>Weapons</th>
<th>Incidents</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide guards with identification, communications device, and any other necessary equipment for the job</td>
<td>Equip guards with non-lethal force and arm them only when justified by SRA</td>
<td>Ensure ability to receive and assess incident reports and other complaints</td>
<td>Ensure appropriate conduct through document review, audits, training, and evaluation of incident reports or complaints</td>
</tr>
</tbody>
</table>
Public Security

Public security → reporting line outside company

5 Questions to Address Public Security Risks

1. What are the types of public security forces involved?
2. What is the number and role of public security personnel involved?
3. What type of public security response is likely to be used?
4. What is the background and track record of these public security forces?
5. How should risks be documented?

Topics for Engagement with Public Security Forces

Engagement
- Personal introductions, willingness to engage, identification of appropriate representatives, establishment of regular meetings

Deployment
- Type and number of guards and the competency, appropriateness, and proportionality of this deployment

Community Relations
- Potential impacts on communities, and any engagement efforts, including grievance mechanism and any known complaints

Use of Force
- Security force deployment and conduct, including desire for preventive and proportional responses

Security Personnel
- Background and reputation of security personnel, to the extent possible, and engagement and monitoring efforts

Training
- Current provision of any training and opportunities to collaborate on capacity building, as appropriate

Equipment
- Existing needs and potential offers, expectations, and conditionality, including implementation of restrictions, controls, and monitoring

Incidents
- Policies and procedures for recording, reporting, and monitoring allegations of unlawful or abusive acts
Elements of an SMP

- Overview of Security Situation
- Physical Security
- Security Operating Procedures
- Security Supervision and Control
- Private Security Force Management
- Managing Relations with Public Security
- Incident Reporting and Inquiry
- Community Engagement and Grievance Mechanism
- Objectives, Mission, and Approach of Company Security
- Company Policies and Standards Relevant to Security
## Assessing Allegations or Incidents

### Key Steps in Assessing Security-Related Allegations or Incidents

<table>
<thead>
<tr>
<th>Key Steps</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record the incident or allegation</td>
<td>Take corrective action to avoid recurrence</td>
</tr>
<tr>
<td>Collect information promptly</td>
<td>Report any unlawful act</td>
</tr>
<tr>
<td>Protect confidentiality</td>
<td>Document the process</td>
</tr>
<tr>
<td>Assess the allegation or incident</td>
<td>Conduct further inquiry, if warranted</td>
</tr>
</tbody>
</table>

Monitor and communicate outcomes
TOOLS AND TEMPLATES

- PDF in Handbook + Word doc downloads
- Additional guidance
- Ready-to-use templates

- Drafting an SMP
- Further Resources

- RFP for SRA/SMP
- Contract w/ Private Security Provider
- Incident Report
- MoU
Providing security is consistent with respect for human rights

Use of force: defensive and proportional responses

Contextual risk is essential but often overlooked

Link between security and community relations is key
Thank You!

www.ifc.org/securityforces