



10 Steps to Maintain Security in Compliance with Human Rights

VOLUNTARY
PRINCIPLES
ON SECURITY + HUMAN RIGHTS

What is the purpose of this tool?

This tool aims to support companies and security professionals in starting their efforts to establish a meaningful security and human rights program that includes implementing the Voluntary Principles on Security and Human Rights (VPSHR), by following **10 steps**:

Step 1: Embed security and human rights into business strategy, governance, plans and budgets	3
Step 2: Analyze and manage security and human rights risks with a focus on conflict prevention	5
Step 3: Proactively engage and work with public security forces.....	8
Step 4: Work with your private security provider.....	10
Step 5: Provide security and human rights training.....	12
Step 6: Implement use of force, weapons, and firearms controls (if relevant).....	13
Step 7: Record, report and investigate allegations or incidents of human rights abuse	15
Step 8: Engage your stakeholders and ensure transparent security arrangements	16
Step 9: Monitor implementation at the business level and corporate level	18
Step 10: Share lessons learned	19

This tool is not intended to be a comprehensive reflection of a VPSHR implementation or security and human rights program, but a brief outline of the key steps that should be included.

How can this tool help your company?



Helps companies to **establish and maintain a meaningful security and human rights program** that is aligned to the business strategy and supported by senior leaders, investors, stakeholders, employees, security partners, and local communities.



Helps companies to **identify and manage security and human rights risks** that could negatively impact people, communities, business operations, reputation, investor confidence, and social license to operate.



Supports implementing the VPSHR and helping business security arrangements protect and respect human rights.



Promotes a security environment where companies, public security forces, private security providers engage and work together to address challenging security situations with a high potential for security and human rights abuse.

What are the key steps in an implementation process?

Each step includes key tasks and available tools to support implementation.

The Voluntary Principles Initiative wishes to acknowledge the hard work of the following individuals, all current or former Members of the Voluntary Principles Initiative, without whom this document would not have been possible: Joel Bisina, Sean Cornelissen, Charles Dumbrille, Jonathan Drimmer, Christopher ‘Mac’ Grace, Elizabeth Kariuki, Trine Pertou Mach, Annie McGee, J.J. Messner, Louisa Petralia, Almero Retief, Fiona Sartain, Helen Simpson, and Leslie Taylor.

Step 1: Embed security and human rights into business strategy, governance, plans and budgets

This step aims to help companies and security professionals establish a security and human rights program that is meaningful, aligned to the business strategy, and supported by senior leaders, investors, internal stakeholders, employees, security partners, and local communities. It also helps establish a governance framework that highlights the company’s commitment to Security and Human Rights (SHR) (inclusive of the VPSHR), as well as the security and human rights requirements and implementation process for business operations.


Key tasks

- 1.1** Secure senior leader/ board buy-in, and a corporate mandate to create a meaningful security and human rights (SHR) program. Have a senior leader act as the Sponsor for the program.

- 1.2** Appoint a Champion to drive the planning, implementing, and maintenance of the SHR program. Depending on the size, scope, and complexity of business operations this could be a part-time, volunteer, full-time, or term position.

- 1.3** Work with the Sponsor and internal stakeholders to develop and agree on the:
 - Broad strategy, approach, objectives, outcomes, and priorities for the SHR program.
 - Position of the SHR program and Champion role within the company.
 - Roles and responsibilities of the SHR Champion.
 - Stakeholders (internal and external), departments, and functions that will engaged (who, why, how, when).
 - Data collection and reporting requirements.

- 1.4** Develop an Annual SHR implementation plan and budget that is aligned to the overall SHR program strategy and business priorities. Consider the following:
 - Results of security and human rights risk assessments (see Step 2)
 - Business priorities
 - Travel costs and time related to field support, stakeholder engagement, and attendance of SHR meetings/workshops
 - Training and awareness raising: Material development, review, translation, printing, production, training-of-trainers, duration, delivery mode, communications, FTE/SME cost, etc.
 - Timing that works for business operations
 - Delivery mode (in-person, remote support, conference call, etc.)
 - Staffing requirements (in-house capability vs use of external SME’s/ consultants)
 - Key tasks, person responsible, deliverables, target date, and costing
 - Guiding business operations on the implementation of security and human rights requirements
 - Key performance indicators and criteria to judge success.



TIP: Coordinate planning with different company departments

To increase effectiveness, consider planning coordination between: Security, Community Relations, Health and Safety, Environment, Human Resources, Procurement, Operations, Legal Counsel, and others.

- 1.5** Work with the Sponsor and stakeholders to develop a public statement of commitment/ endorsement of relevant human rights standards, the Voluntary Principles, engagement with local stakeholders and vulnerable groups, as well as ensuring transparency and accountability around business security and human rights practices:
 - “We will uphold the Universal Declaration of Human Rights, international human rights principles and standards, as well as International Humanitarian Law, wherever we operate”
 - “We are committed to implement the UN Guiding Principles for Business and Human Rights and the VPSHR”
 - “We are committed to analyse and manage security and human rights risks and to work with local communities, indigenous leaders, and vulnerable groups to find meaningful and lasting solutions to any adverse human rights impacts by our business operations”
 - “We are committed to work with private and public security providers on security and human rights issues, and will take the steps necessary to ensure that business security arrangements respect the rule of law and respect human rights”

Key tasks

- 1.6** Incorporate security and human rights commitments and requirements into company governance, behavioral standards, and compliance requirements. For example:
- Develop a company definition of human rights that is linked to the Universal Declaration of Human Rights and international human rights principles
 - Endorse the UN Guiding Principles for Business and Human Rights and company's commitment to implement the VPSHR in its human rights policy
 - Include security and human rights requirements in the company human rights policy, security standard and/or security procedures
 - Highlighting the principles and values of respect, integrity, and transparency in the company code of conduct
 - Develop clear guidelines on the use of force, weapons, and firearms for security purposes
 - Develop SHR self-assessments
-
- 1.7** Develop guidance, tools and training that support SHR implementation. For example:
- **Standards/procedures:** Highlights the SHR requirements that business operations are required to implement and comply with
 - **Guidance:** Elaborates on the requirements and explains how and what business operations are required to do to implement and comply with the SHR requirements
 - **Tools:** Includes templates, examples, or checklists that can be used to do the job
 - **Training:** Builds knowledge, understanding, and the skills required to do the job
-
- 1.8** Develop key messages to support the implementation and maintenance of the SHR program. Prepare to answer the following questions:
- What are the Voluntary Principles on Security and Human Rights (VPSHR)?
 - Why implement the VPSHR?
 - What is the value-add for the company? Why does security and human rights matter?
 - What is the company's commitment and practices in support of (security and) human rights?
 - What are the SHR requirements for the business?
 - What are business operations required to do to ensure compliance (implementation process)?
 - Who can sites contact for support and where can they find more information and tools to help them do the job?
-
- 1.9** Promote awareness of security and human rights practices and requirements throughout the company, including within the value chain. This can be done through presentations, briefings, workshops, employee induction, internal messaging, sharing of best practices, training, reporting, the onboarding of security contractors and sub-contractors, etc.
-



Helpful resources:

[The Voluntary Principles on Security and Human Rights – An Implementation Toolkit for Major Project Sites](#)

(Pages I-1 and VI-1 to VI-4)

[The Voluntary Principles on Security and Human Rights: Backgrounder on Company Implementation](#)

All the resources can be found at voluntaryprinciples.org or online.

Step 2: Analyze and manage security and human rights risks with a focus on conflict prevention

This step aims to help companies identify, analyze, and manage risks, impacts, and the causes of conflict that could negatively impact the companies' ability to protect and respect human rights, or lead to company complicity in human rights abuses.

Key tasks

- 2.1** Initiate the risk process.
- Confirm the company risk methodology, processes, tools, and requirements to be complied with.
 - Define the scope of the risk assessment, business activities, and area of operation.
 - Ensure the scope highlights the risks outlined in 2.2 below.
 - Identify the people, communities, and activities impacted by business arrangements and activities.
 - Incorporate any legal/ regulatory requirements that should be considered.
 - Define the stakeholders, departments and functions to be consulted. For example:
 - Internally: Business Resilience Coordinators; Community Relations; Human Resources; HSE; Operations; Ethics and Integrity; Procurement; Security contractors; Human Rights Advisor; etc.
 - External: Community Leaders/ Representatives; Vulnerable groups; Public security providers; NGO's, etc.
 - Consider stakeholder perceptions / expectations.
 - Identify, collect, and share with stakeholders relevant risk information, including: previous security and human rights risk analyses or impact assessments; country-specific data/risk profile; crime statistics; proliferation of firearms and weapons; presence of armed groups; human rights complaints/grievances; knowledge of security and human rights threats; risks in the external and internal operating environment; human rights records of public and private security providers; results of conflict analysis; etc.
-
- 2.2** Identify sources of security and human rights risk. For example, Module 2: Risk Assessment of the VPSHR, Implementation Guidance Tools (IGT) highlights the following potential sources:
- **Conflict situation:** Recent history of conflict; potential for recurrence of conflict; potential for international conflict; illicit activity (e.g., drug trafficking, smuggling, crime syndicates etc.); insurgency, armed separatist or guerrilla group; unsettled territorial claims; etc. Assess if a conflict is the result of the interactions between multiple actors, including companies, all levels of government, communities, non-governmental organizations (NGOs), insurgents, and criminals.
 - **Security provisioning:** Low level of competence of public security providers; low level of competence of private security providers; low level of resources; poor human rights record by public security providers; low understanding of human rights and humanitarian law by security providers; history of force abuse; culture of impunity; culture of lack of accountability; violations of the rights of vulnerable groups; poor command and control environment and lack of protocols (public or private); etc.
 - **Governance:** Corruption; political instability; weak rule of law; poor governmental capacity; disregard for the rights of minority groups; limitations or repression on press freedoms, media, civil society freedoms; political interference in investigations of human rights abuse; politically-motivated violent attacks on company personnel or assets; etc.
 - **Socio-economics:** Poverty; income or wealth disparity; land or resource conflicts; ethnic or religious tensions; tensions over resettlement; concerns over negative social impacts of company activities (e.g. local inflation, negative impacts on social cohesion, etc.); abuse of Indigenous People's rights; labour concerns; business rivalries; history of community opposition to projects/ business activities; etc.
 - **Physical Environment:** Negative environmental impact (e.g. air, water, soil, etc.) created by company activities; past poor environmental performance by industry; key environmental challenges (e.g. biodiversity, species at risk); etc.
-

Key tasks

- 2.3** Identify security and human rights risks, with special emphasis on:
1. Risks associated with political, economic, civil or social factors.
 2. Potential for violence and conflict.
 3. Human rights records of public security forces, paramilitaries, law enforcement, and private security.
 4. Local prosecuting authority and judiciary's capacity to ensure accountability.
 5. Conflict analysis with identification of the root causes of conflicts and level of adherence to human rights standards.
 6. Risks associated with the transfer of lethal and non-lethal equipment to security providers.
 7. Risks associated with the presence of private and public security forces and operations.
 8. Security risk scenarios with increased potential for public security forces intervention and risk of force abuse (e.g., dealing with protests targeting the business, illegal/artisanal mining, land resettlement, armed attacks on guards and company assets, etc.).
 9. Business practices and activities that may lead to stakeholder conflict situations (e.g. workforce reductions; change in suppliers or supply chain; wage disputes; grant payments/disbursements; not honoring commitments/promises to the community; etc.).
-
- 2.4** Analyze security and human rights risks. This typically involves:
- Using the identified risks to develop clear "risk scenarios" or "risk statements" for analysis.
 - Estimating the consequence (also known as impact) and likelihood (also known as probability) for each of the identified risks.
 - Taking current risk controls and their effectiveness into account for each risk.
 - Use of a 'Heat Map' or 'Risk Matrix' to help categorize and prioritize risks, on the basis of consequence ratings and likelihood ratings (as per the company risk methodology and process).
-
- 2.5** Identify risk treatment and mitigation. This typically involves:
- Deciding how each security and human rights risks will be treated. For example, Module 2: Risk Assessment of the VPSHR, Implementation Guidance Tools (IGT) highlights five options:
 - **Accept it** – Accept the risk as it is
 - **Avoid it** – Do not to undertake the activity that creates the risk
 - **Mitigate it** – Take actions to reduce either the consequence and likelihood (or both) of the risk
 - **Transfer it** – Obtain insurance (Note: may be difficult for many VPSHR risks)
 - **Share it** – Share the risk with another entity (e.g through a contract with a private security provider, or a written agreement with public security forces)
 - Treating risks in order of priority.
 - Assigning a risk owner for each risk.
 - Working with the risk owner to agree the actions/controls, action/control owners, deliverables, timeline, and review dates.
 - Consolidating all risk responses into a Risk Management Plan and presenting to senior management for review and implementation approval.
 - Integrating findings and risk responses into management systems (as required).
-

Key tasks

- 2.6** Communicate, monitor and revise security and human rights risks. This typically involves:
- Regularly engaging with risk owners, control owners, or supporting action owners, to monitor the implementation progress of risk responses.
 - Periodically updating senior management and select risk stakeholders on the status of risk implementation progress and challenges.
 - Reviewing security controls and action status at an agreed frequency.
 - Tracking actions to completion.
 - Ensuring that security and human rights risks, as well as the SHR Risk Management Plan, are updated at least annually, or immediately following a change in security and human rights risk exposure.
-



Helpful resources:

[Module 2: Risk Assessment, Voluntary Principles on Security and Human Rights Implementation Guidance Tools \(IGT\)](#)
(Pages 22 to 35)

[ISO 31000 Risk Management](#)

[Good Practice Handbook – Use of Security Forces: Assessing and Managing Risks and Impacts, Guidance for the Private Sector in Emerging Markets](#) (Pages 17 to 31)

Company risk governance, methodology, and tools

Conflict assessments produced by authoritative and independent organizations, such as the [Heidelberg Institute for International Conflict Research](#)

[Verisk Maplecroft Human Rights Risk Indices](#)

[Human rights due diligence in conflict-affected settings: Guidance for extractive industries](#) (Pages 9 to 45)

[Human rights in the mining and metals industry: Integrating human rights due diligence into corporate risk management processes](#)

All the resources can be found at voluntaryprinciples.org or online.

Step 3: Proactively engage and work with public security forces

This step aims to help companies manage their interactions with and closely work with public security providers to ensure that human rights are protected and respected as part of company security operations.

Key tasks	
3.1	As in Step 2, assess and document the nature of any public security force presence or deployment (either specific to the project or in general) as well as risks arising from the use of public security forces.
3.2	Consider, based on the level of contextual risk, what is an appropriate role and scope for public security forces vis-à-vis the project and identify what aspects of that role and scope the project can influence.
3.3	Consult with host governments and local communities about security arrangements and the impacts on local communities and encourage host governments to make security arrangements transparent.
3.4	Understand and identify the types of public security forces that will respond to different kinds of incidents.
3.5	Understand, based on likely scenarios, what public security actions and activities in and around the project may look like, and what the specific human rights risks from such outcomes may be.
3.6	Research (discreetly) the background and track record of public security forces, particularly in the project area/region.
3.7	Seek to encourage the deployment of individuals who are appropriately trained and have not been implicated in allegations of abuse.
3.8	Work closely with public security forces and local communities to promote understanding of company requirements and practices in support of VPSHR implementation. Designate and define responsibility within the company and/or project on who is authorized to engage with public security forces, and how.
3.9	Engagement with security forces need not be at a “ministerial” level but can often be most effective at the local level. Identify who within the police or military detachment is appropriate with whom to build a relationship with regular or semi-regular engagements on operational matters. Remember that such engagements may require cultivation of long-term relationships to build trust.
3.10	Ensure that all efforts to engage with public security forces are properly and extensively documented, even if unsuccessful.
3.11	Once a relationship is established, identify opportunities to discuss topics such as community relations and equipment, to potentially sensitive topics such as deployment, training, use of force, etc. and to impart company requests on expectations of activities and behaviour.
3.12	Attempt to conduct joint planning on likely scenarios, to better understand how the public security forces may respond to an incident (such as a protest) and to convey expectations on how the project wishes to see such incidents responded to in a legal and responsible manner.
3.13	Consider if there are opportunities to invite public security forces to observe or attend the company’s own internal human rights trainings.
3.14	If public security forces make requests of the project to supply equipment or provide funding, etc., and if the requests are reasonable and legal, ensure that the supply of such support is well documented, including the stated and agreed acceptable use and accountability for all such support.

Key tasks

- 3.15** If public security forces make requests of the project to supply equipment, consider how that leverage can be used to help facilitate discussions on broader issues. Ensure that any support:
- Does not contravene any recognized laws, regulations, or standards.
 - Excludes the loan, transfer, or procurement of security weapons, firearms, or ammunition.
 - Excludes military/tactical police-style training.
-
- 3.16** Develop and implement a process for recording and reporting allegations of abuses by public security forces, monitoring investigations, and pressing for proper resolution.
-
- 3.17** Where force is used by public security, report the incident to the local authorities, and provide medical aid to any injured persons.
-
- 3.18** Attempt to solicit a Memorandum of Understanding with public security forces, a written, signed document that outlines commitments and expectations on critical issues, particularly deployment, training, equipment, and reporting of allegations of abuse.
-



Helpful resources:

[Module 3: Public Security Providers, Voluntary Principles on Security and Human Rights Implementation Guidance Tools \(IGT\)](#) (Pages 36 to 37)

[Good Practice Handbook – Use of Security Forces: Assessing and Managing Risks and Impacts, Guidance for the Private Sector in Emerging Markets](#) (Pages 57 to 76)

[Model Clauses for Agreements Between Government Security Forces and Companies](#)

[Addressing Security and Human Rights Challenges in Complex Environments Toolkit](#) (Pages 39 to 87)

All the resources can be found at voluntaryprinciples.org or online.

Step 4: Work with your private security provider

This step aims to help companies manage their interactions with and closely work with private security providers to ensure that human rights are protected and respected as part of company security operations.

Key tasks

- 4.1** Use the results of needs assessment and Security Risk Assessment (SRA) to inform the type and level of security required (to manage the security risks/threats to people and business operations).
-
- 4.2** Consider which security provider you wish to hire and ensure that the Scope of Work / Terms of Reference accurately reflect the level/type of security required. Equally, consider whether you wish to hire a local company or an international provider – both may have strengths and weaknesses, depending on the context. Key considerations may include host country mandatory requirements, regulatory compliance, local hiring, availability, gender balance, community perceptions and concerns, professionalism, etc.
-
- 4.3** Properly vet selected security providers and make reasonable inquiries as to whether the company is properly licensed, professional, and whether it has been implicated in any past issues, human rights abuse, or wrongful acts. Examine the security provider's procedures, particularly when it comes to hiring, certification, licensing, training of their employees, use of force, and dealing with misconduct.
-
- 4.4** Review the security provider's vetting of employees. Ensure they have processes in place to reasonably guarantee that they are not hiring employees with past records of human rights abuse or criminality.
-
- 4.5** Ensure that the contract with the security provider is robust and includes:
- Reference to adherence to the VPSHR and applicable international guidelines.
 - All expectations and company policies, as well as remedy for violation of those policies.
 - Expectations regarding appropriate conduct and the use of force.
 - Requirement to report and investigate human rights, use of force, and firearm related allegations or incidents.
 - Mandatory weapon and firearm controls (if relevant).
 - Mandatory security and pre-deployment training (in line with country laws and the scope of work), including human rights and use of force training.
 - Performance reviews and compliance checks.
 - A termination provision where there is credible evidence of unlawful or abusive behavior.
-
- 4.6** Review (and even co-create) the security provider's training program and all supporting materials. Key considerations include:
- Is the training program and materials accessible? (i.e., is it in the appropriate language for the guard force) is it appropriately tailored for the level of education?
 - Does the training program meet local legal/regulatory requirements and standards?
 - Does training include use of force (and where appropriate, firearms and first aid training)?
 - Does the training include human rights standards for basic security duties of search, seizure, arrest, protests, dealing with vulnerable groups and victims of crime?
 - Does it include behavioral training, inclusive of respect and conflict de-escalation?
 - Is there any kind of testing component that demonstrates uptake and understanding?
 - Is the training program iterative and does it include refresher training, and if so, how frequently?
-
- 4.7** Consider what policies and procedures will be implemented.
- Will guards be armed/ equipped with firearms? If firearms are to be deployed, is their justification for it in the level of risk assessed by the SRA? Even if firearms are deployed, will they be readily available or stored on an as-needs basis? (See also Step 6)
 - What are the use of force protocols?
 - Will guards be equipped with less-than-lethal weapons and if so what? (See also Step 6)
 - What are the chain of custody protocols for firearms?
 - Will there be a Code of Conduct, and what should it include?
 - What will be the process and response for when an incident and investigation occurs?
-
- 4.8** Designate who shall have responsibility for oversight and monitoring of the security provider – after all, you can contract away your security, but you cannot contract away your responsibility.

Key tasks

- 4.9** Ensure that there is a process in place to log incidents and to be able to receive reports or complaints (both internally and externally) and to put in place a process for reviewing, investigating (if required), and resolving incidents.
-
- 4.10** Work closely with your security provider, supervisors, and frontline guards to promote understanding of company requirements and practices in support of VPSHR implementation.
-
- 4.11** Ensure that any support to armed private security suppliers:
- Does not contravene any recognised laws, regulations, or standards.
 - Excludes the loan, transfer, or procurement of security weapons, firearms, or ammunition.
 - Excludes military/tactical police-style training.
-
- 4.12** Regularly check:
- Security guards to ensure they are appropriately equipped, trained, and licensed.
 - Security provider firearm / weapon handling controls and practices.
 - Security incident reporting and quality.
 - Etc.
-
- 4.13** Involve your security provider in future security and human rights impact assessments.
-
- 4.14** Monitor security supplier performance and work with your supplier to address any gaps in service delivery.
-



Helpful resources:

[Module 4: Private Security Providers, Voluntary Principles on Security and Human Rights Implementation Guidance Tools \(IGT\)](#) (Pages 48 to 57)

[Section III: Working with private security providers, Addressing security and human rights challenges in complex environments](#) (Pages 88 to 144)

[Good Practice Handbook: Use of Security Forces: Assessing and Managing Risks and Impacts, Guidance for the Private Sector in Emerging Markets](#) (Pages 41 to 56)

All the resources can be found at voluntaryprinciples.org or online.

Step 5: Provide security and human rights training

This step aims to help companies plan for the most suitable training for their teams and assists companies in determining which stakeholders they must train.

Key tasks	
5.1	Develop trainings tailored to different audiences based on needs and risks. Incorporate examples that such employees may encounter in carrying out their duties.
5.2	Ensure that the training provides an understanding of security and human rights principles, and likely scenarios that security personnel may face.
5.3	Ensure that training includes particular emphasis on the use of force, and appropriate uses of weaponry that security personnel may receive.
5.4	Consider in particular training regarding handling protests, strikes, human rights defenders, investigations, detention, interfacing with youths, national minorities, and vulnerable populations, and other areas where tensions and human rights impacts may occur.
5.5	Ensure all guards and supervisors are trained in the Voluntary Principles on Security and Human Rights, which provides an understanding of how the principles relates to their work. Similar training can be offered to local public security forces.
5.6	Engage with host governments to ensure that public security personnel receive human rights training by certified trainers during induction and throughout their service.
5.7	Ensure that any military or paramilitary public security personnel receive specific training related to civilian policing, particularly in relation to use of force and legitimate targets.
5.8	Include training for private security personnel requirements and principles surrounding interfacing with public security personnel.
5.9	Provide training to senior business leaders about the value of the security and human rights framework and why applying those standards are helpful to the business.
5.10	Track the trainings delivered, test for comprehension, provide regular updates, refreshers and reminders, and re-train as needed.
5.11	Update training material periodically to capture new developments and new risks.



Helpful resources:

[Module 4: Private Security Providers, Voluntary Principles on Security and Human Rights Implementation Guidance Tools \(IGT\)](#) (Pages 48 to 57)

[Section III: Working with private security providers, Addressing security and human rights challenges in complex environments](#) (Pages 88 to 144)

[Model Clauses for Agreements Between Government Security Forces and Companies](#)
[Voluntary Principles Training Course](#)

All the resources can be found at voluntaryprinciples.org or online.

Step 6: Implement use of force, weapons, and firearms controls (if relevant)

This step aims to ensure that the use of any security weapons and firearms are justified, legal, and strict controls are implemented to manage the use of force, weapons, and firearms in support of company security arrangements.

Key tasks

- | | |
|------------|--|
| 6.1 | Agree with the business leader on the process, criteria, and security risks/ threats that will be used to drive the decision to approve/ not approve the deployment of security weapons and firearms. |
| 6.2 | Confirm with relevant government authorities the types of weapons, firearms, and ammunition that may be used for security services, as well as the regulatory requirements for the business, suppliers of armed security services, and individual armed security personnel. |
| 6.3 | Consider options to reduce the footprint and number of security weapons and firearms deployed (e.g. limiting firearms to patrol vehicles; using an external armed response company instead of full-time deployment of firearms; using a combination of armed vehicle patrols and unarmed guards; etc.). |
| 6.4 | Appoint a point-person responsible for the day-to-day management and control of all security weapons and firearms. |
| 6.5 | Work with the armed security provider to agree on the weapon, firearm and ammunition platform, as well as the use of force continuum that allows for the use of lesser and non-lethal force options, before resorting to the use of lethal force options such as weapons and firearms. |
| 6.6 | Ensure administrative controls are in place to record the issue, make-safe, receipt, safe storage, handing over, use, transportation, and disposal of firearms and ammunition used (e.g. personal pocket books, a security diary/ log, or registers for this purpose (e.g. firearm register, stock and ammunition control register, key register, daily firearm permits, etc.)). |
| 6.7 | <p>Work with the armed security provider to agree on the plan/ procedure/ mechanisms to support strict and effective day-to-day management and control of all weapons, firearms and ammunition, in accordance with domestic laws and including:</p> <ul style="list-style-type: none"> • Secure storage • Designated make-safe area and make-safe instructions for all types of firearms in use • Controls over the issuance of weapons • Records regarding to whom and when weapons were issued • Identification and accounting of all ammunition • Firearm certification and licensing • Verifiable and proper disposal • Mandatory reporting of all use of force, weapons, and firearms (UOFWF) incidents • Recordkeeping procedures to ensure weapons are accurately recorded (e.g. taking down a written account, writing a detailed incident report, filing a report with local law enforcement authorities, reporting on progress and actions taken in support of an incident, compiling an investigation report, etc.) • Mandatory and proper investigation of all UOFWF incidents and full cooperation and support during resulting investigations, inquiries or legal proceedings • A training plan to maintain the proficiency of armed security personnel in human rights, use of force, weapons, firearms, First Aid, and relevant company security policies and procedure • Measures to ensure that weapons and firearms are not handed to any authorized personnel, suspected or known to be under the influence of alcohol, narcotics, medication, or any other substance that may impair his/her judgment • Regular weapon, firearm, and ammunition inspections (e.g., daily, weekly, monthly, and surprise inspections) |
| 6.8 | Keep copies of all documents required to legally and professionally use and be in possession of weapons, firearms or ammunition (e.g., licenses, certificates, and training records) |

Key tasks

- 6.9** Ensure that your weapon and firearm carry systems allow for the safe carry, make-safe, and easy deployment, for example:
- OC spray (mace) is carried in a pouch that is attached to a waist belt system
 - Batons are carried using a ring, or a rotating or break scabbard that is attached to a waist belt system
 - Pistols, revolvers, and accompanying magazines are carried using a waist belt, holster and separate magazine or roll pouch
 - Rifles are carried using a shoulder sling
 - Extra ammunition is carried in a pouch that is attached to a belt system
-
- 6.10** Develop a procedure to guide security personnel in the deployment, first response, and the use of weapons and firearms. This includes, but is not limited to guidance on:
- When and under which conditions weapons and firearms may be issued to security personnel
 - When and under which conditions firearms may be loaded with different types of ammunition and conditions for their use
 - Conditions and options for the use of force
 - When and under which conditions firearms may be issued to security personnel
 - When and under which conditions a firearm may be pointed or discharged (fired) in general, or in self-defense or defense of others
 - Conditions for the use of different types of weapons, firearms and/or ammunition
 - Approaching and dealing with one or multiple armed suspects
 - How weapons and firearms should be carried and transported
 - Firearm stances and conditions for the use of weapons and firearms (as per country law)
 - Ensuring the safety of all persons at the scene of the crime or incident
 - Giving medical assistance/first aid and contacting emergency services for potential injuries
 - Doing an initial assessment of the scene and giving a situation report
 - Alerting Emergency Response Teams (ERT's) and secondary responders
 - Taking all steps necessary to cordon off and restrict access to the incident scene
 - Handing over any crime scene to the first responding police or investigating officer
 - Compiling a basic sketch/taking a photograph of the scene of the incident
 - Ensuring that any firearms, weapons or any other evidence at the scene are not disturbed
 - Identifying any witnesses and recording their details
 - Separating witnesses from one another (if possible and appropriate)
 - Continuing to collect as much information as possible about the incident
 - Taking accurate notes and recording all actions taken
 - Giving a written statement if needed
 - Cooperating in full during any subsequent investigation process
-
- 6.11** Ensure that the contract/Memorandum of Understanding (MoU)/written agreement with armed security providers reference all business requirements, legal requirements, and mandatory controls for the deployment of security weapons and firearms.
-
- 6.12** Work closely with armed private security providers and public security forces (working on site) to ensure that weapon and firearm controls are adequate, efficient, and maintained.
-
- 6.13** Continue to work with local enforcement and firearm regulatory authorities to ensure that armed security providers and armed security personnel deploy security weapons, firearms, and/or ammunition in accordance with country laws.
-
- 6.14** Ensure that security risk analysis and management plans consider the additional risks posed by the deployment of security weapons and firearms (e.g. risk for force abuse, unlawful or unauthorized possession or use of security weapons and firearms, unsafe storage of security weapons and firearms, aggravated assault, etc.).
-



Helpful resources:

[Voluntary Principles Training Course](#). Use of force Continuum. Module 4: Use of Force from a Human Rights Perspective
All the resources can be found at voluntaryprinciples.org or online.

Step 7: Record, report and investigate allegations or incidents of human rights abuse

This step aims to assist companies in developing mechanisms to record and track allegations and incidents of human rights abuses, to provide clear direction on who should be notified if an allegation is made, and to help companies with steps to be taken after the completion of an investigation.

Key tasks

7.1	Ensure you have an incident management system which allows you to track allegations, reports, and investigations.
7.2	Implement formal operational grievance mechanism, and identify and publicize pathways to raise grievances, with appropriate review and escalation.
7.3	Ensure a procedure and system is in place to support mandatory reporting and independent investigation (as necessary) of all incidents or allegations related to: <ul style="list-style-type: none"> • Security and human rights abuses. • Violations of international humanitarian law. • Discharge, accidental discharge, pointing, injury, damage, allegations of unsafe or unauthorised use, force abuse, or legal inquiry resulting from the use of security weapons, firearms, or dogs.
7.4	Develop clear reporting path within both security function and business team, which includes regular reporting and pattern analysis to detect potential trends. Also develop clear guidelines for when matters need to be reported externally.
7.5	Conduct an internal investigation. <ul style="list-style-type: none"> • Respect confidentiality to the extent practicable. • Share findings with stakeholders. • Assess next steps.
7.6	If the allegation requires external (e.g., police) investigation, support that investigation and reporting, monitor its progress, and encourage appropriate resolution.
7.7	Consider disciplinary steps for private security personnel or employees, or engagement with public security around continued deployment of implicated personnel.
7.8	Assess whether the company caused or contributed to a negative impact, such that it would be appropriate to participate in remedy processes, or whether it is directly linked to a negative impact, such that it should use its leverage with a third party to provide appropriate remedy.
7.9	Use the results of investigations to agree on improvement actions to limit, reduce, prevent, or deter reoccurrence of such an allegation or incident at the relevant site and other locations, or caused by the company’s business relationships.



Helpful resources:

- [Effective Operational-Level Grievance Mechanisms](#)
- [Site-Level Grievance and Community Response Mechanisms: A Practical Design and Implementation Guide for the Resource Development Industry](#)

All the resources can be found at voluntaryprinciples.org or online.

Step 8: Engage your stakeholders and ensure transparent security arrangements

This step aims to help companies develop meaningful engagement with various stakeholders with different and sometimes contradictory interests to ensure that different viewpoints are heard and that the input is used in decision-making.

Key tasks

- 8.1** Undertake rigorous stakeholder identification to develop a comprehensive list of all stakeholders relevant to your operations. These should include: those who make decisions (relevant government agencies and offices in home and host states); those who implement them (public security, third party/contracted private security, executive management and other relevant staff in the company implementing VPSHR and regulatory institutions at the home and host states); those who are impacted by them (communities); and interested parties (civil society organisations/ social movements/interest groups etc). Be rigorous: communities themselves comprise of various stakeholders (e.g. religious groups, women's groups, leaders, youth groups, elders, and less visible groups) that may not be represented only by the most visible, be mindful of the less visible or outspoken.
-
- 8.2.** Give special attention to societal norms (e.g., gender norms), inequalities and vulnerabilities and adopt engagement mechanisms that ensure that you engage all segments of the community, including the most vulnerable. This might entail holding separate meetings with the women and youth in the case of a highly patriarchal society, or even separate meetings for persons with disability in a community where this category of people is highly excluded from decision-making.
-
- 8.3.** Stakeholders beyond the direct project footprint must be considered. The activity(ies) may have a positive impact on a directly-affected community but may entrench inter-ethnic or intra-community divisions and drive conflict if other communities perceive they are not benefiting from the project, or are negatively affected by it.
-
- 8.4** Identify and analyze interests of the above categories of stakeholders in relation to your operations and the extent to which these interests diverge or converge. Impacts may differ from group to group. Ensure that you always remain impartial.
-
- 8.5** Identify the capacity, strengths and weakness/vulnerabilities of each of the stakeholders. Strengths could include: access to information, clout and influence and requisite skills to engage, whereas weakness and vulnerabilities could include: fear of victimization by community members and workers, lack of information, language barrier, etc.
- Through the stakeholder consultation process stakeholders can be put at risk and the most vulnerable stakeholders may be marginalised without representation. However, if these stakeholders are not consulted, it is possible the project will lead to further marginalisation and potentially violent conflict.
-
- 8.6** Based on 5.4, outline the skills, information and other support that you need to provide to the different stakeholders to enable them to effectively and meaningfully engage.
-
- 8.7** Identify the most suitable platforms and mechanisms for engagement for the different stakeholders based on the issues that you need to engage them on. To ascertain suitability of engagement platforms, consider their access and conduciveness to facilitate open conversations. Additionally, consider the objectives of engagement in order to decide on the most appropriate platforms and mechanisms to use. The objectives could include:
- Risk and impact assessment process, including contextual analysis.
 - Influencing policy processes.
 - Consensus Building.
 - Dialogue.
 - Influencing decision making.
 - Engaging your contractors on your commitment to the VPSHR and their role in the implementation of the Principles.
 - Grievance handling.
 - Sharing information, creating awareness and capacity building.
 - Monitoring implementation of the VPSHR and the impact on the ground.
-
- 8.8** Designate the role of driving and managing stakeholder engagement to a suitable office and personnel, preferably within the Social team. Stakeholder consultations in FCS require a dedication of time and resources, provision of safe and accessible spaces, and sufficient time should be allowed to ensure that consultations are meaningful, for example if necessary trust-building and capacity-building is required.

Key tasks

- 8.9** Forge cross-departmental synergies to ensure that stakeholder engagement is pro-active and is infused in key operational process. This includes collaboration between the Security and Social Departments of your company to address and resolve any grievances.
-
- 8.10** Document any grievances that arise from stakeholder engagement and escalate the same to the relevant office/offices for resolution.
-
- 8.11** Maintain a good relationship with stakeholders and create a conducive environment for them to call for meetings and set/propose the agenda.
-
- 8.12** Manage stakeholder expectations from the on-set through being transparent and forthright about what your company can deliver and what it cannot. This is especially important in relation to employment and procurement opportunities as well as social services and infrastructure that the host national government and local government are supposed to deliver e.g healthcare, water, road maintenance etc. In the case of corporate social responsibility (CSR) projects, be open about your internal CSR policy and strategy and whenever possible, engage communities in identification and prioritization of projects so that your CSR projects are responsive to local needs. Ensure that your CSR projects are inclusive and non-discriminatory so that they do not cause divisions and tensions.
-

- 8.13** For every issue and/or engagement ensure that you:
- Provide full information in a timely manner to your stakeholders so as to address the problem of power asymmetry and enable them to effectively engage.
 - Genuinely seek the opinion and consent of stakeholders before undertaking critical actions that may adversely affect them.
 - Act on or incorporate the views and recommendations of your stakeholders in your decision making.
 - Convene feedback meetings to update stakeholders on the progress of implementation of actions jointly agreed upon and any other relevant updates. These forums also present you with an opportunity to get feedback on the utility and effectiveness of stakeholder engagement and other actions.

Where relevant and possible, ensure that your stakeholders have the requisite technical capacity to effectively engage on technical matters, for example, providing them with legal support in negotiating land acquisition and understanding contractual documents.

The above tasks are very important in making stakeholder engagement processes meaningful to both your company and your stakeholders, creating ownership among stakeholders and limiting the likelihood of mistrust and conflicts.



Helpful resources:

[Module 1: Stakeholder Engagement, Voluntary Principles on Security and Human Rights Implementation Guidance Tools \(IGT\)](#) (Pages 10 to 21)

[Addressing Security and Human Rights Challenges in Complex Environments Toolkit](#) (Pages 15 to 38; 145 to 196)

[Human Rights Defenders' Toolbox](#) (Pages 55 to 64)

All the resources can be found at voluntaryprinciples.org or online.

Step 9: Monitor implementation at the business level and corporate level

This step aims to ensure that companies and security professionals actively monitor SHR implementation at all levels of the company and that any improvement actions are recorded and tracked to completion. Stakeholders (internally and externally) should also be informed and updated on Security and Human Rights (SHR) implementation efforts.

Key tasks

- 9.1** At the business level, have the person responsible for security:
 - Meet regularly with private and public security providers to review security and human rights risks, discuss service delivery, and compliance with security and human rights requirements
 - Conduct compliance checks on private security providers and security operations
 - Work with private and public security providers to agree actions to address gaps or performance deficiencies
 - Conduct audit or assessment of implementation of the security and human rights program, including adherence to the VPSHR, company policies, and local laws
 - Report to senior leaders and the corporate SHR Champion on implementation, incidents, issues, opportunities, and lessons learned
 - Review weapons logs, use of force reports, training logs, detention reports, licenses, investigation reports, and other relevant documents for adherence to company policies, program requirements, and relevant laws

- 9.2** At the company level, have the SHR Champion report to senior leaders on the implementation of the SHR program, with emphasis on:
 - Implementation progress (against the objectives and outcomes of the program)
 - Challenges and proposed solutions
 - Best practices
 - Lessons learned (see Step 10)
 - Opportunities
 - Next steps

- 9.3** At the business and company level, any human rights improvement actions need to be recorded and tracked to completion.

- 9.4** Consider adopting organizationally appropriate KPIs and tracking relevant metrics, consistent with the VPSHR model KPIs.

- 9.5** Keep record of all SHR related engagements, incidents, and actions taken.

- 9.6** Keep stakeholders (internal and external) informed of company SHR efforts and progress.

- 9.7** Report on company SHR implementation (as required).



Helpful resources:

[Voluntary Principles on Security and Human Rights: Performance Indicators](#)
[Auditing Implementation of Voluntary Principles on Security and Human Rights – A Guidance Document to Assist Companies and their Auditors Assess Implementation of the Voluntary Principles on Security and Human Rights](#) (Pages 31 to 42)

All the resources can be found at voluntaryprinciples.org or online.

Step 10: Share lessons learned

This step aims to ensure that companies and security professionals capture and share lessons learned and best practices both internally and externally, to prevent other companies and security providers repeating the same security and human rights mistakes, and to take advantage of security and human rights best practices.

Key tasks

- 10.1** Document and share lessons learned and best practices with senior leaders, persons responsible for security, security providers, security personnel, subsidiaries and joint ventures, and stakeholders.
- 10.2** Share lessons learned and best practice with Voluntary Principles Initiative peers and networks, including in annual reports and verification presentations.
- 10.3** Include lessons in relevant training programs, implementation working groups, and share with local communities (as relevant).
- 10.4** Participate in local and international panels, discussions and roundtables where the VPSHR, and relevant lessons, can be shared.



Helpful resources:

[Auditing Implementation of Voluntary Principles on Security and Human Rights – A Guidance Document to Assist Companies and their Auditors Assess Implementation of the Voluntary Principles on Security and Human Rights](#) (Pages 40 to 42)

All the resources can be found at voluntaryprinciples.org or online.

Who we are

The Voluntary Principles on Security and Human Rights are an internationally recognized set of principles that guide companies on how to conduct their security operations while ensuring respect for human rights. The Voluntary Principles Initiative (VPI) is a multi-stakeholder initiative dedicated to sharing best practices and mutually supporting the implementation of the Principles.