Guidance on Developing Security Management Plans to Implement International Security Standards and the Voluntary Principles

February 14, 2019
Version 1.0

Introduction

This document provides guidance for developing a Security Management Plan (SMP) that supports implementation of the Voluntary Principles on Security and Human Rights (VPSHR), and the application of other international best practices. This information represents the best practices and practical experience of MSWG members gained from applying these measures around the world.

The Mining Security Working Group (MSWG) was established in 2015 as a forum for subject matter experts and security practitioners within the extractive industry to collaborate and share insights and learnings of ongoing challenges, technological advances, best practices, and further the goals of industry initiatives such as the Voluntary Principles on Security and Human Rights and UN Declaration of Human Rights.

There are many documents, available from a variety of sources, that address implementation of the VPSHR. They all discuss the need for polices and procedures that support the principles, but an organization must have a strong security foundation to ensure the success of the implementation process.

The MSWG is proud to support the initiatives of the Government of Canada, the Mining Association of Canada, and extractives industry leaders in promoting respect for human rights. We welcome the opportunity to share our collective security management experience with both practitioners and those assigned responsibility for security oversight.

Scope

Implementation and application of the VPSHR's requires an organization to conduct Threat and Risk Assessments, develop department standards for proprietary and contract security, and carefully consider their relationship with, and support for, public security. To accomplish this, a well considered security management plan that follows industry best practices is required.

A Security Management Plan (SMP) is a document that outlines the organization's security philosophy, strategies, goals, programs, and processes. It provides strategic guidance for the security department's development and direction in a manner that is consistent with the company's overall business plan. It should also outline risk assessment and mitigation plans.

The SMP guides the company's actions in mitigating and protecting against risks of a security and human rights nature that could threaten communities, employees, facilities, operations, production, the reputation of the company and its global operations.

An important consideration of SMP development is aligning the mission and strategies of the security program with those of the organization. This ensures that the security function is not seen just as an expense, but is an integral part of the business and contributes to an environment of success.

The SMP is a tool that helps the security manager achieve agreement and buy-in from other business units. It articulates how the security department interrelates and supports all areas of the organization.

A well written plan provides direction, organization, integration and continuity to the security program. It demonstrates knowledge of the risks and thoughtful response planning.

The SMP is a strategic document. Whereas, a Site Security Plans (SSP) is a tactical document and is the logical extension of a SMP. The SSP articulates the specifics of physical security, guard force responsibilities, relations with public security and other components of security service delivery. Additional guidance on SSP development can be found in Appendix A of this document.

Security Management Plan Development

1. Principles of Security Management

Unity of Effort: Security management efforts should be a collaborative effort within the organization and should include input from all partners and stakeholders both internal and external.

Transparency: Information on how risk mitigation decisions are made should be shared with those that have a valid need to know.

Adaptability: Strategies and processes should be designed to allow for constant change.

Practicality: Security Managers cannot predict the future, nor can they eliminate all threats. They must be practical in what they choose to protect and evaluate the cost/ benefit of countermeasures.

Customization: Solutions must meet the needs and respect the culture of the organization.

2. Developing a Blueprint

Management input on establishing security goals is imperative and should include service delivery expectations and core duties.

The security management framework should enhance preparedness, response, resilience, and support business continuity. Development of an SMP should include:

- Policy Commitment
- Alignment with the organization's strategic objectives
- Legal and International Standards Requirements
- Organizational Profile (Mission, Production, Strategies)
- Risk Assessment - Internal and External Context
- Stakeholder Concerns
- Development of Plans and Budgets
- Security Personnel, Infrastructure Requirements and Interdependencies
- Security Options (countermeasure analysis)
- Cost/Benefit Analysis
- Assignment of Responsibility and Authority

3. Security Management

The security department should approach its mission with the understanding that good security and respect for the human rights of employees and communities are fully compatible. This should be articulated in a comprehensive management policy and plan that includes:

- A management policy commitment to conformance with international best practices for security management and voluntary standards such as the VPSHR.

- A commitment to prevent and reduce the likelihood and consequences of human rights violations.

- Responsibility and accountability for international best practices, such as the Voluntary Principles on Security and Human Rights (VPSHR) delegated to the security manager.

- Communication of the plan to all employees, and available to all stakeholders.

- Alignment with other policies (such as Ethics, Code of Conduct, Human Rights)
- Implementation and review framework for objectives, targets, and programs.
- Commitment to compliance with applicable legal and regulatory requirements.
- Response mechanism to allegations received via Grievance or Whistleblower Hotline.

4. Risk Management

Risk analysis is used to develop proactive and proportionate security plans that reduce the likelihood, probability and consequences of disruptive events. Security threat and risk assessments are prerequisites to determine the deployment of armed or unarmed security forces in support of the organization.

The goal is to develop a comprehensive and systematic process to pre-emptively mange the risk associated with business and security operations. Consideration must also be given to the impact of the organization's activities on the communities in the area of influence. A key challenge is how to proactively manage identified risks, particularly in areas of weak governance, where the human or naturally caused events have undermined the rule of law.

Incident response planning and testing must be aligned with this process and include the development of training exercises, evaluation of protections in place, response protocols, mitigation requirements, recovery capabilities and current operational procedures.

5. Risk Assessment

A risk assessment is an exercise intended to identify security threats, evaluate the nature and extent of the risk posed by those threats, and potential vulnerabilities. Risk assessment assists management in selecting and prioritizing effective control measures. The goals of the risk assessment are to prevent unauthorized activity and the loss of assets, equipment, property, and reputation.

a. Establishing the External Context

Understanding the external context of the organization is essential to ensure the objectives and concerns of external stakeholders are considered when conducting a risk assessment. Assessment should encompass an organization-wide context, consider legal and regulatory requirements, and stakeholder perceptions.

The potential for conflict is inherent in mining and should be recognized and evaluated as part of the risk assessment process. Conflict is often the result of the interactions between multiple actors including companies, all levels of government, communities, non-governmental organizations (NGO's), insurgents, and criminals. The root causes of conflict are complex and may have historical origins.

Evaluation of the external context should include conflict assessment produced by authoritative and independent organizations, such as the Heidelberg Institute for International Conflict Research. Operations in difficult environments must consider whether they have the right policies and systems in place to fulfill corporate obligations and responsibilities. The goal is to avoid causing, supporting or benefiting unlawful armed conflict, contributing to human rights abuses, and breaches of international humanitarian law.

The external context should include, but is not limited to:

- The actions of people outside the project who seek to take advantage of the opportunities presented by the development and operation of the company.
- Common criminal activity.
- Disruption of the project for economic, political, or social objectives; deliberate actions that have a negative impact on the efficient and safe operation of the company.
- Risks associated with the presence of private and public security forces and operations.
- Social, cultural, political, legal, regulatory, financial, technological, economic, natural and
  competitive environment, whether international, national, regional or local.
- Key drivers and trends that could impact on the objectives of the organization.
- Relationships with, perceptions and values of external stakeholders.
- In extreme cases- terrorism, armed insurgency, coups, or war and the risks that a security response might produce.

b. Establishing the Internal Context

The internal context considers the operating environment in which the organization seeks to achieve its objectives. The risk management process should be aligned with the organization's culture, processes, structure and strategy.

Internal context is anything within the organization that influences the way in which an
organization will manage risk, and should consider:

- The objectives and mission of the organization.
- The potential for illegal, unethical, or inappropriate behaviour of project personnel or those directly affiliated with it.
- Common risks such as employee theft, workplace violence, labour unrest, and sabotage.
- Risks to employees or others associated with security response.

c. Risk Gap Analysis

Before beginning the process of managing risk, an understanding of the various interconnected contextual elements that affect the organization must be developed. Risk gap analysis helps establish the context and should include:

- Identification of applicable legal requirements and international standards.
- Evaluation of existing risk management practices and procedures, including those associated with subcontractors and supply chain.
- Evaluation of previous emergencies and incidents, along with the measures taken to prevent and respond.
- Risk identification, preventative measures, corrective measures, and recommendations for improvement.

6. Policy and Procedures

An organization should not assume that a security contractor will develop the policies, objectives, and procedures needed to protect their business, people, assets, and reputation. Management must take responsibility for determining the level of security required, identifying the assets to be protected, and support the implementation of security countermeasures. This responsibility should be documented and reviewed regularly, along with contractor performance.

Governance of the SMP should consider:

- Senior management accountability.
- Roles and responsibilities for all aspects of the SMP, including requirements, development, review, training, continuous improvement, and approval.
- Responsibility and resourcing for the management of the SMP.
- A security policy that articulates direction, accountability, authority, and oversight for the SMP.
- Implementation and awareness training for all employees to ensure maximum effective use of the SMP.

A Security Policy is a high-level document, signed by the CEO or other senior executives that outlines the company's vision for securing its people, assets, and reputation. The document demonstrates management's commitment to security and is a directive on 'what' the company wants to be accomplished.

The security policy covers all company offices and operations, and informs all managers of their responsibilities. This is a brief document that articulates broad concepts. It is the responsibility of the security manager to develop guidelines and procedures that explain 'how' the policy will be fulfilled.

Guidelines and procedures define and explain the actions required to assure conformance to the policy. Ideally, they eliminate any single point of failure, or subjective interpretation. They define mandatory compliance and will form the basis of induction and recurrent training for security staff and employees.

a. Records

A key part of security management is the maintenance of administrative records that includes:

- Contracts with private security providers
- MOU's and material support documentation with public security
- Risk Assessment and Analysis
- Internal compliance reviews
- Equipment accountability
- Weapons authorizations
- Licensing
- Training
- Access Controls
- Secure storage of sensitive information
- Code of conduct and Ethics attestations
- Applicable International, National, and local laws
- All formal or informal public commitments made by the organization

b. Responsibility, Authority, and Job Descriptions

Responsibilities, authority, and job descriptions must be clearly articulated in the SMP. The SMP must be reviewed and signed by the responsible executive or senior manager to whom the security manager reports. These documents should include responsibility to document and report all interaction with public security, contractors, public authorities, and community representatives.

The organization should strive to attract and retain security personnel with the skill, knowledge, and ability to implement the desired level of security. As the greatest contributor to poor performance is a lack of training the organization should commit to the professional development of security personnel to improve job performance, service delivery, reduce complaints, and increase retention.

7. Security Supervision and Control

The SMP must outline the department structure and responsibility, and articulate:

- Lines of control, accountability, and supervision for the security department.
- Supervision of the front-line guard force.
- Responsibility for security information sharing and communication.

The SMP should outline the planning and coordination activities between security and other departments (Community Relations, Human Resources, and Government Relations) and business units, which may involve participation in security risk assessments to regular meetings.

It is important to ensure that all security activities are coordinated and supervised through a single point of control and command, and operate within consistent guidelines and procedures. Security cannot be effective if it serves two masters.

See **Appendix A**, Bridging Security Management and Site Security Plans, for connecting the strategic management plan with department operations best practices.

Key Reference Documents

Reference 1

Voluntary Principles on Security and Human Rights. Audit Protocol to Assess Compliance with Key Performance Indicators (June 2013)

https://www.business-humanrights.org/sites/default/files/media/documents/voluntary-principles-audit-protocol-jun-2013.pdf

Requires an organization to prepare:

- Statement of commitment or endorsement of the VPSHR.
- Relevant policies, procedures, and/or guidelines (or any changes thereto from the previous reporting year) for implementing the Voluntary Principles.
- Security and human rights risk assessments.
- Procedure and mechanism to report security-related incidents with human rights implications by public/private security forces relating to the company's activities.
- Include the VPSHR when entering into relations or contracts with public/private security providers.
- Address security related incidents with human rights implications by public/private security forces relating to the company's activities.

- Apply VPSHR standards in the selection of private security providers, formulation of contractual agreement with private security providers, and all arrangements with public security forces.

Reference 2

International Finance Corporation Performance Standard 4 (Community, Health, Safety, and Security)

https://www.ifc.org/wps/wcm/connect/a40bc60049a78f49b80efaa8c6a8312a/PS4_English_2012.pdf?MOD=AJPERES

Requires companies to:

- Assess the security risk their operations may have or could create for communities.
- Develop ways to manage and mitigate these risks.
- Manage private security responsibly.
- Engage with public security.
- Consider and investigate allegations of unlawful acts by security personnel.

Also:

- Understand the organization's risk, security, and human rights protection requirements.
- Establish polices and objectives to manage risk.
- Implement operating controls to manage risk, security measures, and respect for human rights.
- Monitor and review the performance and effectiveness of security plans (administration and operations).
- Promote continuous improvement based on object measure.

Reference 3

IFC Good Practice Handbook, Use of Security Forces: Assessing and Managing Risks and Impacts, Guidance for the Private Sector in Emerging Markets

https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces

- **Managing Private Security**

Decisions regarding the type, number, responsibilities, and arming of private security forces should flow from an assessment of the security risks and appropriate responses.

- **Equipping**

Do guards have what they need to do their jobs properly and safely? This usually means a uniform, identification, and a 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 is a serious one that should derive from the assessment of risk and be accompanied by a dedicated training program.

- **Vetting**

Who is 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 the appropriate use of force**

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**

Training should focus on appropriate behaviour 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.

- **Monitoring**

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. Companies contracting security services still retain oversight responsibility of third-party security providers to ensure appropriate vetting, use of force, training, equipping, and monitoring of guards.

- **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 armed forces. 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: When are public security forces likely to be involved? (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**

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 the 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**

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).

- **Threat and Risk Assessment**

Research and analysis of the country context: Consideration of potential risk in the broader operating environment may include inherent country risk, the rule of law, criminality, physical environment, socioeconomic context, governance, conflict situation, and industry-specific information that could affect the security situation. In addition to country-specific risk, it is also advisable to review the strength and reputation of existing public security forces.

Research and analysis of the national and/or local security situation: Analysis of the security situation often considers the availability and professional reputation of private security, track record and human rights reputation of public security forces (such as police or military), and any other significant elements in a company's particular circumstances.

- **Prevention and Mitigation Measures**

Developing and refining prevention and mitigation measures often requires consideration of how to address the wider range of potential impacts coming out of the scenarios, including a prioritization process. The risk response chart and heat map may assist a company in determining which risks and impacts to address as the highest priority. Including Community Relations staff in the design of mitigation measures can increase their overall effectiveness.

Chapter V of this document (*Preparing a Security Management Plan*) provides a broad outline for security management plans.

Reference 4

Other Reference Documents

- ANSI/ ASIS RA1.2015 Risk Assessment Standard:

  https://webstore.ansi.org/Standards/ASIS/ANSIASISRIMSRA2015

- ANSI/ ASIS Management System for Quality of Private Security Company Operations: http://www.acq.osd.mil/log/ps/.psc.html/7_Management_System_for_Quality.pdf

- ASIS General Risk Assessment Guideline:

- https://www.asisonline.org/publications/sg-asis-general-security-risk-assessment-guideline/

- ASIS Private Security Officer Selection and Training:

  https://www.asisonline.org/publications/sg-asis-private-security-officer-selection-and-training-guideline-2010-ed/

- Auditing Implementation of the VPSHR, Global Compact Network Canada: http://www.globalcompact.ca/auditing-implementation-of-the-voluntary-principles-on-security-and-human-rights/

- Contemporary Security Management (John Fay, Elsevier):

  https://www.elsevier.com/books/contemporary-security-management/fay/978-0-12-381549-1

- ICMM https://www.icmm.com/en-gb/publications/mining-and-communities/voluntary-principles-on-security-and-human-rights-implementation-guidance-tools

- ICRC and DCAF's Security and Human Rights Toolkit: http://www.securityhumanrightshub.org/content/toolkit

- International Association of Oil and Gas Producer's Report on Firearms and the Use of Force: http://www.ogp.org.uk/pubs/320.pdf

- International Code of Conduct for Private Security Service Providers:

  www.icoca.ch/

- MIGA's Implementation Toolkit for Major Project Sites: https://www.miga.org/documents/vpshr_toolkit_v3.pdf

- OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas:

http://www.oecd.org/corporate/mne/mining.htm

- Risk Analysis and Security Countermeasure Selection (Thomas Norman, CRC Press):

  https://www.crcpress.com/Risk-Analysis-and-Security-Countermeasure-Selection-Second-Edition/Norman-CPPPSPCSC/p/book/9781482244199

- Risk Analysis and the Security Survey (James Broder, Elsevier):

  https://www.elsevier.com/books/risk-analysis-and-the-security-survey/broder/978-0-12-382233-8

- UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials: www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx

- UN Code of Conduct for Law Enforcement Officials: www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx

- Voluntary Principles on Security and Human Rights: http://www.voluntaryprinciples.org/resources/

- Voluntary Principles Implementation Guidance Tool:

  http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/VPs_IGT_Final_13-09-11.pdf (English)

  http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/IGT-SPANISH1.pdf (Spanish)

- World Gold Council Conflict-free Gold Standard https://www.gold.org/who-we-are/our-members/responsible-gold/conflict-free-gold-standard

APPENDIX A

Bridging Security Management and Site Security Plans

1. Private Security Force Management

The role of private security is to provide preventive and defensive services, protecting company employees, facilities, equipment, and operations. Private security personnel have no law-enforcement authority and must not encroach on the duties and responsibilities reserved for public security forces.

a. Contract Security

A contract provides the legal basis for the relationship between the organization and the security contractor. The organization is responsible for all activities outsourced to another entity, and requires constant oversight and supervision. Responsibility to respect human rights and comply with the law cannot be sub-contracted to a third party. The organization is ultimately responsible for the actions of a contractor.

The contract should specify the responsibilities, terms, and conditions under which the contractor is to provide security services. The contract should clearly define:

- A commitment to abide by the same obligations as held by the company.
- Confidentiality and conflict of interest requirements.
- A process for assessing risk and reporting undesirable and disruptive events.
- Description of the services to be performed by the contractor.
- The requirement for human rights training prior to entering into service.
- The mechanisms in place to ensure that physical force is only used when strictly necessary and to an extent proportional to the threat.

b. Selection of Private Security Contractor

In selecting a security provider, the organization must perform proper due diligence that includes screening for institutional reputation, training standards, procedures for screening employees, and any history of allegations of human rights abuses or other criminal behaviour.

Only retain the services of competent security contractors committed to operating in a manner consistent with human rights standards, such as the VPSHR. The organization is responsible and liable for the contractor's work and personnel. You cannot sub-contract away the responsibility to respect human rights.

The organization should establish and document the criteria for screening and selecting contract security. It is the responsibility of the organization to ensure the contract conforms to applicable laws and all other contractual obligations. Potential contract security providers must be investigated to ensure:

- A demonstrated history of carrying out security activities in compliance with relevant laws.
- Their ability to protect the client's people, property, and reputation.
- Adequate resources and qualified personnel are provided to meet operational objectives.
- Transparency, accountability, and adequate supervision of their personnel.
- All financial, statutory, and renumeration benefits for their personnel are fulfilled.

- Requisite registrations, licenses, and permits are current.
- Accurate personnel and equipment records are maintained.

c. Active Oversight of Contractor Performance

To ensure proper performance, the organization must undertake regular audits, assist with training, inquire into any credible allegations of abuse or wrongdoing, and monitor performance on an ongoing basis.

d. Selection, Background Screening, and Vetting of Security Personnel

Security personnel occupy positions of confidence. The company should establish documented procedures for pre-employment background checks and vetting. Minimum standards must be established and procedures implemented to screen out applicants who do not meet the qualifications based on their knowledge, skills, abilities, and experience. This selection process must form part of all contracting to ensure no person credibly implicated in human rights abuse is hired.

Additionally, valid background checks must be completed on potential security providers to screen for allegations of past abuses, inappropriate use of force, or other criminal activity and wrongdoing.

The screening and vetting process should be based on the nature of the job for which the candidate is being considered, the person's level of authority, and area of specialization. Screening should take place before a candidate is offered a position and starts work. Candidates should sign the proper authorizations and consents before performing background screening.

Security personnel with access to sensitive information and operations should be subjected to more stringent background checks.

Privacy and confidentiality of all personal information must be protected.

e. Security Guard Background Screening

Verification of identity and personal history should include:

- Home address check
- Employment records
- Electronic media
- Criminal and civil records history
- Human rights violations
- Motor vehicle records
- Credit report

- Sexual offender database
- Government and industry sanction
- Industry licensing records

f. Verifying Experience and Qualifications

Experience and qualification verification should consider, but is not limited to, the following:

- Education
- Employment history
- Licensing/ Certification/ Registration
- Personal references
- Supervisor and co-worker interviews
- Military/Police service

Exclusions, unavailable, unreliable, or unsuitable information should be documented.

g. Screening and Vetting

Establish clearly defined criteria to evaluate:

- Substance abuse.
- Physical and mental fitness.
- Suitability to carry weapons.
- Resilience to stressful and adverse conditions.
- Criminal association and susceptibility to corruption.

h. Competence, Training and Suitability

The greatest contributor to poor performance is a lack of training.

The security department should identify the knowledge and skills required by proprietary and contract staff to perform the tasks assigned. The department should establish its own minimum induction training standard as national or regional standards may not meet the requisite competencies. Induction training must always be completed before entering into service. Contractors must demonstrate that their employees have received and satisfactorily completed the training. Monitoring and recurrent training should be conducted on an ongoing basis to identify opportunities for improvement and demonstrate due diligence.

The SMP should commit the organization to maintain the highest standards of guard-force technical and professional proficiency through a comprehensive training program. SSP's should outline the training responsibilities of both the security provider and the company and the annual schedule.

Training should include respect for human rights, grievance mechanisms, ethical conduct, Use of Force, and competence with issued offensive and defensive weapons. Practical, scenario-based training that reinforces decision making in conditions that reflect the operating environment is recommended. Training should include procedures for prevention and mitigation, response, incident documentation, communication, and accountability.

The company should review contractor training programs and, where necessary, augment the training through the use of qualified third parties or direct instruction. At a minimum, security personnel should receive induction and recurrent training in:

- Basic guarding skills
- Guard-post orders and procedures
- Code of Conduct, Ethics, and Human Rights
- Use of Force
- Health, Safety, and Environment
- Use of defensive and offensive weapons (as applicable)

All weapons training should be conducted to a written standard appropriate for the weapons issued. Training should include scenario-based training, mechanical and operation training that includes malfunctions, and live fire qualification. Training should be conducted not less than annually, and more frequently if required by law.

2. Use of Force

The use of force by private security is only sanctioned for preventive and defensive purposes in proportion to the nature and extent of the threat.

When necessary to arm the guard force, the organization will ensure high levels of technical and professional proficiency and a clear understanding of the rules for the use of force. This requires recurrent training on the Use of Force guidelines, proportionally, and respect for human rights.

The authorization to carry weapons should only be given to qualified personnel in accordance with the terms and conditions of a contract. Weapons should be issued only after the background and qualifications of personnel have been established, and training on the specific weapon issued has been satisfactorily completed. This should only be authorized when there is a reasonable expectation of threat to life based on risk assessment. Weapons training, deployment, and necessity to carry must comply with host country law. Evaluation of the necessity to deploy weapons consider the possible consequences of accidental or indiscriminate use of weapons.

Use of force must always be reasonably necessary, proportional, and lawful. Rules for the use of force must be reviewed to ensure they meet the appropriate national or regional legal standard. Options for non-lethal, less-lethal, and lethal force must be considered in the local context and legal requirements.

Use of force rules should be outlined in all contracts with private security providers. Contract provisions should include:

- Parameters for the use of physical force.
- The circumstances under which persons are authorized to carry weapons, and the weapons and munition permitted.
- A commitment to ensure weapons are only used in appropriate circumstances and in a manner likely to decrease the risk of unnecessary harm.
- Prohibition of the use of unauthorized weapons and munition.
- Regulations for the control, storage, and accountability of issued weapons.
- Graduated response guidelines on the use of force.
- Emphasize the use of de-escalation techniques.
- A reporting mechanism for all use of force incident.

a. Use of Force Training

Rules on the use of force must be incorporated into both induction and recurrent training programs. Records of training and demonstrated competence are to be maintained. Use of force training should emphasize:

- The use of lethal force only in circumstances of self-defence or defence of others against the imminent threat of death or serious injury, never to be used in defence of property;
- Force should be reasonably necessary, and used as a last resort;
- Force should be proportionate to the threat, and only deployed based on the totality of the circumstance to counter a threat;
- Use of force is only used to attain lawful objectives.

Training on a use of force continuum should outline, but is not limited to:

- Security presence;
- Verbal commands;

- Open-hand controls;
- Non-lethal weapons;
- The threat of lethal force;
- Use of lethal force.

Use of force training must reinforce the premise that private security is not a substitute for public security and reinforce the limitations of their authority.

Training programs must emphasize that lethal force is justified only under conditions of extreme necessity, and as a last resort when all lesser means have failed or cannot reasonably be employed. Lethal force is only to be used in self-defence in the defence of others, or when it reasonably appears necessary to prevent the commission of a serious offence involving grave threat to life or serious bodily harm.

The defence of others may include the use of lethal force when it is reasonably necessary to prevent the theft or sabotage of inherently dangerous property, the loss or destruction of which would present an imminent threat of death or serious bodily harm. The legal authority may also authorize the use of lethal force if it reasonably appears to be necessary to prevent the sabotage or destruction of critical infrastructure, the damage to which would create an imminent threat of death or serious bodily harm or injury.

b. Management of Weapons and Munitions

The security department is responsible for establishing, maintaining, and documenting procedures that ensure:

- All weapons and munition are acquired lawfully;
- Constant accountability for all weapons and munition issued and returned;
- Weapons and munition issued are proportionate to the risks identified and tasks to be performed, and meet all legal standards;
- Appropriate provisions are made for storage, issue, and maintenance;
- Contractors deploy only weapons and munition approved by the organization;

All persons authorized to carry a weapon have a valid license and current training.

c. Apprehension and Detention of Criminals

As part of the Use of Force training, security personnel must be trained on how to deal with persons apprehended or detained in the course of executing their duties. They must understand the limits of their authority and that this will typically only include person interdicted during an attack on personnel and property under their lawful protection. Training should emphasize the requirement to treat apprehended personnel humanely and respect their human and constitutional rights.

Training will include measures for protecting the apprehended person from violence, and immediate reporting and transfer to competent authorities. Incident reports must be prepared that includes the person's identity, alleged offence, to whom they were transferred, first aid or assistance provided, and their condition at the time of transfer.

Persons detained may be searched by security staff to ensure their safety against weapons and to safeguard evidence. Search procedures must ensure the dignity and humane treatment of the detainee, and will distinguish between minimally invasive and comprehensive searches.

All persons detained should receive immediate first aid as required.

3. Uniforms

All security team members should adopt the use of uniforms that indicate their department affiliation. Private security uniforms and equipment, such as patrol vehicles, should be of a pattern, colour, and markings that distinguish them from public security. Security staff and vehicles should have unique badge numbers that facilitate identification and enables transparent reporting.

Uniforms project a positive image about the organization and encourage professional and responsible conduct. There may be s circumstances where a risk assessment indicates it is advisable to use non-uniformed security. When a discreet approach is required security personnel should not openly carry firearms and maintain on their persons non-transferable identification.

The presence of uniformed security is the first option on every use of force continuum. Uniforms and marked vehicles indicate to employees, the public, and public security that team members have authorization and responsibility to protect company personnel and assets.

4. Communication

Effective communication is the most important component in preventing, managing, and reporting security events. Communication plans ensure adequate control, coordination, and functionality for security operations.

The SMP should outline communication procedures and processes that consider:

- Internal communications within departments, contractors, clients, and stakeholders;
- Receiving, documenting, and responding to communications from external sources;

- Structured communication with public security and emergency responders;
- Dedicated and secure communication during disruptive and emergency events.

The organization should establish and communicate its internal and external complaints and grievance procedures. Security personnel must be trained to receive and report complaints and grievances and ensure confidentiality. Unreported and unresolved complaints from the community can quickly become disruptive events.

5. Occupational Health and Safety

A SMP should commit to providing security staff with a safe and healthy working environment, recognizing the inherent dangers presented by the environment and duties. It should emphasize the reasonable precautions to be undertaken to protect all persons working on behalf of the organization, particularly those in high-risk positions, such as security.

6. Incident Response Management

An appropriate administrative structure should be implemented to deal with incident management and response effectively. The SMP should articulate the department management structure, authority for decisions, responsibility for implementation, and reporting. The organization should have an Incident Management Team (IMT) to lead event response under clear direction of management or their delegates. The SMP should outline the role of security within the IMT and include:

- Planning
- Incident response management
- Human resource management
- Health, safety, and medical response
- Information management
- Internal and external communications
- Critical support functions

7. Incident Response

The security department is responsible for developing incident response and management protocols as part of the company risk assessment process. Incident response and management must consider:

- Safeguarding life, property, and reputation of the organization.
- Respect for human rights and human dignity.

- Identification and reporting of potentially disruptive events, mitigation and recovery plans.
- Notification and mobilization procedures for management, stakeholders, and authorities.

The organization should develop procedures for reporting and investigating incidents that includes:

- Time and location.
- The identity of persons involved, including contact information.
- Injuries and damage sustained.
- Circumstances leading up to the event.
- Response measures deployed.
- Cause of all internal and external injuries and damage.
- Root cause analysis.
- Corrective and preventative actions.

The SMP and SSP should outline responsibilities and timelines for conducting inquiries on allegations
and incidents, including:

- A commitment to an expeditious inquiry into any allegations of abuse or wrongdoing.
- Private security contractor conducting investigations into incidents or allegations, and the reserved right of the organization to conduct an independent inquiry.
- Inquiry findings will include a recommendation of appropriate disciplinary action and policy or procedure changes.

8. Performance Evaluation and Continual Improvement

Performance evaluation involves the measurement, monitoring, and evaluation of the department and contractor service delivery, quality assurance, legal compliance, and respect for human rights. Metrics include adherence to policies, and objectives, and performance targets.

Performance indicators should be developed to measure both the management system and operational compliance. Indicators should provide useful information that identifies both successes and areas requiring improvement. They should also identify how significant risks are being managed.

Evaluation should consider:

- Validation of management plans and physical security strategies.
- Competence of security personnel.
- Response capabilities.
- Contract compliance.
- Training and preparedness.

The SMP and SSP should indicate that corrective action will be identified and communicated in a timely manner and should address root cause failure. Responsibility for corrective action and a completion date should be assigned. Findings that exceed expectations should be noted as best practices and shared across the organization.

Continual improvement should consider changes in risks, activities, and operations that effect service delivery. Procedures, systems, and training must be adapted to address:

- Policy changes.
- Changes to hazards, risks and threats.
- Personnel and contract changes.
- Process and technology changes.
- Lessons learned from exercises and training.
- Lessons learned from disruptive events.
- Changes to the external environment (such as political, social, legal).

9. Managing Relations with Public Security

Public security forces have the sole responsibility for responding to and investigating criminal activity, particularly incidents in the public interest. They also have the primary responsibility for public order, including protests, demonstrations and civil disobedience. For incidents involving criminal violations, potentially violent confrontations, or demonstrations, they may be requested to respond to protect company personnel and property. It is important that public security be briefed on the organization’s policies and commitments before they are deployed to an incident.

The company should maintain constructive relations and good communication with public security forces. If public security forces are assigned to the project, it is important that an MOU be established to ensure transparency. The MOU should describe provisions for equipment transfers, material support, and the role of the public security force in protecting company assets. Joint contingency planning, and coordination mechanisms should be developed.