STANDARD GUIDANCE

(COP 11) Security

A. Definitions and applicability

Security personnel are formally employed or contracted to protect property, assets and/or people.

The **Use of Security Personnel** section of the COP is applicable to Facilities that handle Jewellery Products and/or use security guards or engage public or private security providers for security services or support.

Implementation of provision 11.3 regarding Voluntary Principles on Security and Human Rights is applicable to Members with Mining Facilities and should be implemented in conjunction with the **Human Rights** provision of the COP. Implementation of 11.4 is applicable to Members that provide secure transport services to the Jewellery supply chain.

B. Issue background

As acknowledged by the Voluntary Principles on Security and Human Rights, security is a fundamental need, shared by individuals, communities, businesses, and governments alike.

Security is relevant to all parts the jewellery supply chain. Diamonds, gold and platinum group metals are high value materials that can be targeted by criminal elements for financial gain. The resulting risks for personal safety and property require that responsible measures be put in place to minimise security threats. Unfortunately, some kinds to security measures, including security personnel, can in some circumstances raise other types of risks, which must be managed.

The primary role of security personnel is the protection of the company's people, property, product and reputation. Whilst carrying out this role, security personnel require a wide range of procedures and associated training to ensure that security is provided in an effective and responsible manner. In some cases, security personnel are trained to enforce company rules, though under the Code of Practices this should not include disciplining employees. At all times, and particularly when armed, security personnel should use the minimum force proportionate to a threat.

Ongoing social unrest and conflict create a very difficult environment for business. Company personnel, assets or strategic facilities can be the target for violent action. In these situations, private security forces will often be used to protect people and property. Where justified by threat and risk assessments, public security may also be engaged to provide security support.

Some public security organisations have a troublesome history, particularly in repressive societies. There are many documented cases where public security forces have been implicated in serious human rights abuses, or have pursued corrupt policies or practices. There have been examples where public security groups engaged to protect personnel and assets have become involved in corrupt activity, profit from criminal activity, resort to inappropriate use of force or firearms, or otherwise create conflict.

Companies have a legitimate responsibility to staff and shareholders to ensure that their personnel and property are protected from violent or illegal acts. Security threats can emanate from criminal groups, local communities, company employees, illegal artisanal miners and migrant workers. Potential security threats include:

- General theft
- Fraud
- Violent disturbances
- Sabotage of pipelines and other installations
- Illegal mining (armed entry to a mine to steal ore)
- Organized theft of fuel and other commodities

- Organized theft of ore or product (gold/platinum/diamonds)
- Kidnapping, intimidation or assassination of staff.

The security strategy deployed by the company will have an impact on all stakeholders, both internal and external. To avoid increasing the potential for conflict, a security strategy must be risk based and for Members with Mining Facilities, include compliance with the Voluntary Principles on Security and Human Rights.

Public security

Although governments have the primary role of maintaining law and order, security and respect for human rights, companies have an interest in ensuring that actions taken by public security, such as the police and military, are consistent with the protection and promotion of human rights. In some cases where there is a need to supplement private security, companies may be required or expected to contribute to the costs of protecting company facilities and personnel borne by public security. While public security is expected to act in a manner consistent with local and national laws as well as with human rights standards and international humanitarian law, abuses may nevertheless occur.

In particular, mining operations in some locations may have police and/or military personnel protecting mine property or concessions who are located on site, using mine facilities or otherwise supported by the mine. In these situations, the potential for corruption, conflict and political violence is increased and companies must be vigilant to the risks of human rights abuses. While the issues can be complex, companies should seek commitment to the Voluntary Principles on Security and Human Rights in formal agreements with governments, wherever possible.

C. Key initiatives

International standards and initiatives

The Voluntary Principles on Security and Human Rights were developed through collaboration between four national governments, non-government organisations, and companies in the energy and extractive sectors. The Principles seek to guide companies in maintaining the safety and security of their operations within a framework of respect for human rights and fundamental freedoms. The Principles fall into three categories: risk assessment; relations with public security; and relations with private security. They call for a regularly updated security risk assessment, and the engagement of local communities in security issues. The Principles stipulate that private security should provide only preventative and defensive services and should not engage in activities exclusively the responsibility of state military or law enforcement authorities.

International Alert, in collaboration with companies, governments, inter-governmental agencies and other NGOs, has developed a guide to Conflict-Sensitive Business Practices for extractive industries from pre-feasibility to closure. It provides guidance and toolkits for doing business in societies at risk of conflict for field managers working across a range of business activities, as well as headquarters staff in political risk, security, external relations and social performance departments.

The International Code of Conduct for Private Security Service Providers (ICoC) articulates principles for private service providers in accordance with international humanitarian law and international human rights standards. These include rules for the use of force, prohibitions on torture, human trafficking and other human rights abuses, and specific commitments regarding the management and governance of companies, including how they vet personnel and subcontractors, manage weapons and handle grievances internally. The ICOC stems from the "Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict".

National law

Most countries have legislation and regulation regarding the appropriate role of security and military forces in the society. Many national and state jurisdictions require training and licenses for carrying weapons such as firearms, batons or pepper sprays. Police or military certification may be required for certain security duties.

D. Suggested implementation approach

- ***COP 11.1: Security Measures:*** *Members shall establish measures that assess security Risks and protect against product theft, damage or substitution of products within the premises and during shipments. Product security measures shall prioritise the protection of Employees, Contractors, Visitors and personnel employed by other relevant Business Partners.*
  Points to consider:
  - Responsibility for managing security should fall to a senior management function.
  - A security risk assessment should be conducted in order to understand the overall security risk environment. The assessment should identify:
    - types of threats, the level of exposure to these threats, and weaknesses and vulnerabilities.
    - security risks from a broad range of perspectives, including political, economic, civil, social or environmental factors where applicable.
    - potential for human rights abuse through the application of the security measures.
  - Establish processes that can identify structural and emergent security threats and address them at various levels, including effective security management strategies and, where relevant, through community engagement activities. This could include as appropriate:
    - Security policies and procedures that clearly place priority on the protection of people over the protection of product.
    - Training for employees and contractors working at the Member's facilities on relevant security policies and procedures.
    - Internal control procedures to enable rapid detection of theft, should it occur.
    - Appropriate arrangements for security during shipments and for protection of security personnel involved in transportation.
    - Relationships with local law enforcement agencies, where appropriate.
    - Regular consultation with host governments and local communities about the impact of their security arrangements on those communities, where appropriate.
  - Sensitive security-related documentation should be strictly controlled and protected. Auditors may not always be able to have access to the specifics of security measures, as part of the business' risk control, but interviews and observation can be used to determine that the security measures are appropriate.

- ***COP 11.2: Security personnel:*** *Members shall ensure that all security personnel respect the Human Rights and dignity of all people and use force only when strictly necessary and the minimum proportionate to the threat.*
  Points to consider:
  - A written policy or agreement should be established on the conduct of security personnel that establishes the importance of respect for human rights, the boundaries for security activities, appropriate procedures for managing security issues and conflicts, and the consequences of any human rights abuses.
  - Arrangements should be in place for monitoring performance against the policy, and for investigations and disciplinary actions.
  - Certain situations and activities may require that security personnel be armed, and this may be determined by the security provider in accordance with their own risk assessments. Any armed personnel must be properly trained and licenced in accordance with Applicable Law.

- ***COP 11.3: Voluntary Principles on Security and Human Rights***: *Members with Mining Facilities shall ensure that security personnel receive training on and operate in accordance with the Voluntary Principles on Security and Human Rights (2000). The human rights of any Artisanal and Small-Scale Mining (ASM) should be explicitly addressed in training of private security personnel.*
  Points to consider:
  - Implementation Guidance Tools are available from the Voluntary Principles website.
    - Note that security risk assessments should include risks relating to interactions between the mining facilities and any local artisanal and small-scale miners (ASM).

Training of security personnel should specifically include policies for conduct when interacting with ASM and with local communities generally.

- Public security providers:
  - Arrangements for engagement with public security providers should be in accordance with the Voluntary Principles section on 'Interactions between Companies and Public Security'.
  - This should include communication of policies regarding ethical conduct and human rights, and expression of the Member's expectation that security be provided in a manner consistent with those policies by personnel with adequate and effective training.
- Private security providers:
  - Agreements with private security providers should include reference to the principles outlined in the Voluntary Principles section on 'Interactions between Companies and Private Security'.
  - Agreement should include requirements for adequate and effective training of personnel on the relevant principles, and on the Member's policies regarding appropriate conduct and the local use of force, such as through 'rules of engagement'.
- In-house security personnel:
  - Equivalent requirements should apply to any in-house security personnel.
- Records should be kept on training delivered to all security personnel.
- Monitoring arrangements should be established to ensure that policies and requirements are adhered to and allegations of non-compliance are investigated, and reported where appropriate.

- ***COP 11.4: International Code of Conduct for Private Security Service Providers (ICoC):*** *Members whose business is to provide secure transport services to the Jewellery supply chain shall be a signatory to the International Code of Conduct for Private Security Service Providers (ICoC).*
  Points to consider:
  - Under the ICoC, signatory companies commit to operate in accordance with the Code and to respect the human rights of, and fulfil humanitarian responsibilities towards, all those affected by their business activities.
  - The ICoC itself creates no legal obligations and no legal liabilities on the signatory companies, beyond those which already exist under national or international law.

Check:

- ✓ Have you assessed security risks and do you have appropriate security measures in place based on those risks?
- ✓ Do the security measures prioritise the protection of people?
- ✓ Do security personnel know the expectations of their conduct?
- ✓ Members in the Mining Sector: Are security personnel trained on and operate in accordance with the Voluntary Principles on Security and Human Rights?
- ✓ Members that provide secure transport services: Are you a signatory to the International Code of Conduct for Private Security Service Providers?

E. Further information

The following websites have further information on the use of security personnel and conflict situations:

- Business and Human Rights Resource Centre
  www.business-humanrights.org/
- International Alert – Implementation of Conflict Sensitive Business Practice
  www.international-alert.org/our-work/implementation-conflict-sensitive-business-practice-csbp
- International Business Leaders Forum
  www.iblf.org/

- International Code of Conduct for Private Security Service Providers (ICoC)
  www.icoc-psp.org/
- International Committee of the Red Cross (ICRC) – Resource Centre
  www.icrc.org/eng/resources/index.jsp
- Montreaux Document on private military and security companies
  www.eda.admin.ch/psc
- OECD - Risk Awareness Tool for Multinational Enterprises in Weak Governance Zones (2006)
- www.oecd.org/daf/inv/mne/weakgovernancezones-riskawarenesstoolformultinationalenterprises-oecd.htm
- OECD Watch Fact Sheet 3 - Assessing Adherence to the OECD Guidelines' Human Rights Provisions
  http://oecdwatch.org/publications-en/Publication_2402
- Voluntary Principles on Security and Human Rights
  www.voluntaryprinciples.org/
- Voluntary Principles on Security and Human Rights Implementation Guidance Tools
  www.voluntaryprinciples.org/files/VPs_IGT_Final_13-09-11.pdf