GLOBAL SECURITY POLICY

<table>
<thead>
<tr>
<th>DESIGNATION</th>
<th>NAME</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPILED BY:</td>
<td>VP – GLOBAL SECURITY</td>
<td>BRIAN GONZALVES</td>
<td>ORIGINAL SIGNED</td>
</tr>
<tr>
<td>AUTHORISED BY:</td>
<td>EVP – SUSTAINABILITY</td>
<td>THERO SETILOANE</td>
<td>ORIGINAL SIGNED</td>
</tr>
</tbody>
</table>

DESCRIPTION OF CHANGE:

Version 1.0

Index

1. Introduction
2. Purpose
3. Accountability
4. Policy Statements
5. Effective Date
6. Custodian
7. Review
8. Communication

AngloGold Ashanti
1. **INTRODUCTION**

There are myriad internal and external risks for a Security Function to contend with and combined with increasing global developments in communications and technologies, we face greater complexity and uncertainty in our current context. Continuous change and growing trends in the countries in which we operate – such as political instability, unrest, corruption, conflict, terrorism and organized crime among others – all potentially impact the sustainability of AngloGold Ashanti’s business and operations, and compromise our security position.

These challenges and our ability or inability to manage them pose immediate and unacceptable threats to our employees, local communities, associates, assets, revenue, reputation, social license and competitive advantage. They are as pervasive internally, among employees and various business partners across the supply chain, where unethical and dishonest behaviours, actions and practices exist and must be addressed.

In translating our business philosophy, Our Business is People, and the broader Business Sustainability strategy, the core purpose of the security function is to **identify, analyse, interpret and support the business to mitigate security risks, to help drive the value creation pathway for AngloGold Ashanti to become the leading mining company.**

2. **PURPOSE**

In support of the Company, Business Sustainability and Global Security strategies; this policy documents policy statements derived from the Global Security Framework and the associated processes, which is the foundation for implementing security best practice across the global portfolio.

It is expected that Regional, Country and Operational Management ensure compliance to this policy and associated standards, through the implementation of the Global Security framework. Adherence to the policy will:

- limit exposure of harm to our people
- limit our exposure to gold theft
- limit our exposure to theft of company assets
- limit exposure to reputational risk and liability
- contribute positively to the profitability and image of the company
3. ACCOUNTABILITY

This policy applies to all company managed operations and exploration sites and covers the following global security framework processes:

- Duty of Care Security
- Asset Protection
- Crisis Management
- Voluntary Principles on Security and Human Rights
- Policy, Standards and Compliance
- Training and Education
- Technology Management
- Risk Management
- Resource Management
- Operations Center and Software

The Vice President – Global Security is the custodian of this policy and has direct accountability for ensuring that regional and operational management are made aware and understand the purpose of the policy and related standards.

4. POLICY STATEMENTS

- All offices, assets and employees are safeguarded and employees feel safe. Key executives, families of frequent travelers are adequately protected at residences. The Security department knows which executives and travelers, globally, are traveling to high(er) risk areas, informing them of their relative risks and takes action to mitigate those risks. Technology is optimized.

- Incorporating the best use of available resources, reduce the loss of gold to well below the industry average, and within company tolerances. By using intelligence and investigative methods, we know our enemy and its modus operandi around and on our mines, driving our proactive and agile allocation of security resources. Loss of assets is detected, reported, investigated, recovered and appropriate disciplinary and or criminal action taken.
• A fully functional crisis management process whereby incidents, emergencies, disasters and ongoing / imminent crisis are communicated vertically within management, within the prescribed timelines. Issues are resolved in the most efficient way possible, at the proper level, involving “experts” and managers, with the knowledge (and consent where necessary) of corporate Executives. Establishes appropriate levels of decision making authority for all levels during a crisis. CM / IM / ER exercises are conducted bi-annually within regions and at corporate.

• All Security personnel are trained and knowledgeable of the VPS&HR and their obligations. Global Security knows and has had final approval of all security components using weapons. Use of weapons is supported by appropriate threat and risk assessments. Units carrying weapons are adequately trained, and have appropriated rules of engagement. Use of Less Lethal weapons has been introduced and properly applied to applicable mine/exploration sites. Contracts and payments are managed and transparent. Violations of procedures are reported and investigated promptly. VPSHR security process is connected to, consistent with and aligned to aspects managed by Sustainability.

• All aspects of security management have been identified, and grouped into logical processes and sub processes. Global Security has drafted standards for each process or sub process, which includes clear measures of performance. Regional and local procedures are formed to be consistent with corporate policy and standards. Compliance is monitored via a security audit process and reported to relevant stakeholders.

• The security department has a professional development plan to recruit, train and retain the best and brightest security professionals across our entire portfolio. Professional development builds upon current “excellence” in certain areas of management, includes x-training of skill sets and tailors our approach based upon our unique profile – gold mining. Plan includes training to company standards, and educating our security service providers regarding our expectations of service and professionalism as we move toward outsourcing non-core functions.

• Use of technology at separate mines, exploration sites and corporate offices is tied to a central strategy and plan. The use of cameras, sensors, software, monitoring equipment and all technology is compatible. Purchasing is centrally regulated to ensure best use of resources, and to minimize obsolescence. Technology plan is tied to security manpower survey, and facilitates the net reduction of manpower across our portfolio.
• Security Managers generate continuous information and analysis on security risks at all mines and exploration sites. Risks are appropriately mitigated. Information is rapidly communicated to local, regional and corporate managers, to improve decision making. Executives know when and where to halt or scale back operations and why. Corporate risk manager has access to security risk information, which uses same quantitative methods.

• Total global security related spending is known and within tolerances. Security manpower is continuously assessed and allocated based upon threat and risk. Excess manpower is reduced, replaced with technology (where applicable), and outsourced. Contracts for all security services are centrally managed to provide economics of scale, and performances clauses included. Key hires are centrally reviewed for ability / competency. Organization continues to improve efficiency via MOE and ROI.

• Centralised operation centers provides 24/7 coverage to our global portfolio of mines and exploration sites for inflow of information. Operators are trained and skilled in threat and risk assessment, crisis and incident management and familiar with duty of care components. They are equipped with appropriate software that facilitates vertical and horizontal communication of security, safety, community, environmental and human rights information to executives and management.

5. EFFECTIVE DATE

This policy is effective from the date it is signed.

6. CUSTODIAN

The custodian of this policy is the Vice President – Global Security

7. REVIEW

The policy will be reviewed annually

8. COMMUNICATION

The policy will be communicated to the Security Manager at each Operation for appropriate action and distribution. Copies will be provided to the EVP’S, relevant SVP’s, VP’S and General Managers/Managing Directors.