Security

Why is this Group Standard important?	This standard defines the minimum requirements for identifying and managing security risk, to protect AGA's people, assets and facilities and ensure that our people feel safe and protected while undertaking tasks on behalf of the company.
Audience	Anyone responsible for managing, implementing and monitoring the security of AGA's people, assets and facilities.
Legend	*Glossary terms* are in italics. ***Approvals*** are in Appendix 1. Hyperlink to another document or to an intranet site or website. *Reference* to another AGA document without a hyperlink.

You must comply with AGA Group-wide Standards to the extent they apply

Security Risk Management

We anticipate, identify, interpret and monitor security risks at all our locations, implement controls to mitigate the risks and communicate to inform decision-making.

- Identify, evaluate, mitigate and report potential security risks using a risk bowtie methodology to inform whether the risks are Terminated, Treated, Transferred or Tolerated.
- Continuously monitor security risks and update the security threat and risk assessment annually, or when a material change in risk occurs.
- Communicate material changes (for example, increased threat to people, assets and or facilities) in security risks immediately to the relevant:
  - Managing Director or General Manager (for an Operation)
  - Project Director (for a major project / exploration) or Country Manager
  - Business Unit Head of Security and
  - Group Head of Security and Human Rights.

Threat and risk assessment

- Use the threat assessment process to identify and evaluate the sources of potential security risk. Quantify the sources of security risk and examine their characteristics, capability and intentions towards company interests (people, assets and reputation).
- Use iSIMS to evaluate the site's security threats and review on an annual basis, or if there is a material change in risk.
- Complete a risk identification process to identify the nature and sources of risk that could impact people, assets and reputation, and must consider natural, intentional and unintentional events such as malevolent, criminal, social/political events etc. Update annually or in the event of a material change in risk.
- Record the top 15 security risks, control measures and control effectiveness in iSIMS using the bow tie methodology and review annually or if there is a material change in risk.
- Submit, once a week, any significant international, regional, national, or local events and / or crime that could potentially impact (negative or positive) the operation from a security perspective through the online Security Report Centre.
- Review and update the Security Risk Scorecards quarterly to verify accuracy of risk ratings (probability and impact) for the Top 15 Security risks.
- Conflict Risk Barometer assessments (CRB) must be managed using the online CRB Tool, completed and must be reviewed on a monthly basis or when there is a material change in risk.
- Complete a Security 5 Point Plan assessment annually or if there is a material change in risk.
- Provide information to Group Security upon request to support the external compliance requirements related to security risk, such as Conflict Free Gold Standard, World Gold Council Responsible Gold Mining Principles and the International Council on Mining and Metals, Performance Expectations.

Security Risk Mitigation

- Resource security requirements to effectively mitigate risk (removing people from risk, and risk from people), and maximize efficiencies through optimization and integration of people and technical systems.
- Implement mitigating measures using AGA project management principles.
- Complete frequent vulnerability checks (daily / weekly / monthly), based on the type of control measures, using iSIMS to test and verify if required security control measures are in place and functioning to an optimal level, to mitigate risk.

Incident management

- Complete analysis on all security information that influences risk (for example, crime incidents) to determine trends and allow for identification of required security response and mitigating measures to be implemented.
- Record all crime-related incidents and identified non-crime incidents in iSIMS.
- Use the incident type and severity classification criteria in iSIMS for notification of incidents or events.
- Complete a review / investigation (utilizing the Incident Investigation Program (IIP) methodology) on all significant Incidents classified as High, Major or Extreme on the Security Incident Classification Criteria to:
  - determine the basic cause(s), including but not limited to the Security discipline
  - identify and implement mitigating measures and/or corrective action to prevent a similar incident from happening or to minimise the impact such an incident could affect
  - get endorsement of the report and proposed actions from Group Security prior to finalisation.
- Complete an annual self-assessment against all Security group procedures.

Voluntary Principles on Security & Human Rights (VPSHR)

Our commitment to the VPSHR and respect for human rights is the key driver in our security management practices and governs how we identify the potential for conflict, rules of engagement, use of force and transparency in agreements with security forces.

- Assess the risk of conflict and manage interaction with private security and public security in accordance with the *Security VPSHR Group Procedure*.
- Complete and document threat and risk assessments for the protection of people and assets, detailing the potential for conflict, associated risks, and level of security required to mitigate risk.
- Get ***approval*** (Appendix 1 ***ID#1***) for the use of lethal and/or less lethal weapons by any security service provider, including AGA security departments, private or public security services, and provide the completed threat and risk assessment that demonstrates a requirement for use of weapons and that the operating jurisdiction permits the possession of firearms and less lethal weaponry.

- Establish and implement standard operating procedures to ensure that security personnel comply with applicable laws and regulations of the operating jurisdiction and the VPSHR.
- Verify the training and qualifications of security personnel assigned to protection duties and/or carrying out high-risk security activities.
- Provide pre-deployment and annual refresher training, using an accredited training provider, to all security units. Ensure the training covers:
  - use of applicable weaponry
  - minimum use of force
  - rules of engagement
  - their obligation to act in accordance with the VPSHR.
- Establish transparent memorandums of understanding (MOUs) with security forces, getting endorsement from Group Security and Group Compliance and manage relationships through service level agreements.
- Document and retain a copy of all agreements with security forces and maintain an audit trail of equipment transfers (ownership; authorisation; use; tracking and monitoring of equipment; exception reporting) in accordance with agreed MOUs.
- Require security officers to immediately notify, through their chain of command, the application of any use of force, any associated injuries or potential liability.
- Complete an incident investigation in accordance with the *Investigations Group Standard*, as soon as practicable, to investigate:
  - non-compliance with established security procedures
  - injuries and/or fatalities due to security intervention and/or illegal activity
  - potential human rights violations due to security intervention and/or illegal activity.
- Record all potential human rights violations in the VPSHR Registry in iSIMS as soon as practicable.

Security Measures

We implement security measures to ensure that our people are always protected and feel safe, protect our assets and facilities and to minimise potential loss resulting from security breaches.

- Develop, implement and review annually or a material change in risk a Security Management Plan for each site, including:
  - plans for responding to potential security breaches
  - contingency plans to address regional and local issues that affect the security and safety of our people and assets
  - security contingencies, proportionate to the specific risk environment, for site evacuation, isolation, lock-down or lock-out.
- Manage perimeter security, access control, intrusion detection and surveillance, movement and exit of people and vehicles, monitoring and controlling assets leaving company property on a

temporary or permanent basis, and the protection of assets and products in accordance with the *Metallurgy Security* and *Mining Security Group Procedures*.

- Implement and continuously monitor the security protocols in the *Technical Security Group Procedure* regarding use of technology to protect people and assets, including video and audio surveillance, sensors, control rooms and software, monitoring equipment, and other available commercially available security technologies. Allocate security resources (including human, technical, vehicles, security equipment) based on the threats and risks identified in the security risk assessment, and in accordance with the *Security Health of Discipline Group Procedure*. Use technology, where practicable, to remove people from risk and risk from people.
- Establish and implement standard operating procedures for monitoring, tracking and managing the security of our people.
- Provide security awareness briefings and manage the security of offices, residences and travel in accordance with the security protocols documented in the *Security Duty of Care Group Procedure*.

Appendix 1: Authorities

Authority Title		Endorse	Approve	Inform
ID#1 Use of lethal and/or less lethal weapons by any security service provider				
	Vice President, Group Security and Human Rights		✓	

Notes: *Authorities must not be within the same reporting line. That is, a role does not endorse their line management's decisions.*

E ***Endorse:*** *Reviews proposals and provides advice before the approver makes the decision. This role is accountable for the advice given (as opposed to a 'review' or 'checkpoint' in a process). Endorsement is not a right of veto. If an endorser disagrees with a decision to approve, they should escalate as necessary.*

A ***Approve:*** *Accountable for the decision, considering input from the endorser. Majority should have one approver only (single-point accountability).*

I ***Inform:*** *Required to act based on the decision made. Should exclude 'process / courtesy' informs.*