Vedanta Resources Plc

Sustainability Governance System

Technical Standard

Security Management

Technical Standard – Security Management

Standard Title:	**Security Management**	**Date of Revision**	30/01/2021
Standard:	VED/CORP/SUST/TS 15	**Revision:**	v.2

Document Issue and Revision History		
DATE	**REVISION NUMBER**	**CHANGE SUMMARY**
10/02/2012	1	Initial issue.
30/01/2021	2	Signatory Update

Authorised by:	Andrew Lewin
Signature	
Position:	Group Head HSE and Sustainability

Technical Standard – Security Management

Contents **Page**

Technical Standard – Security Management

1. INTRODUCTION

The purpose of this Technical Standard is to ensure that Vedanta manages security risks to its personnel and physical assets and that these risks are managed in a structured and systematic manner that ensures the health and safety of Vedanta employees and others; and that supports our policies in relation to sustainability and protection of the environment. This Standard supports Vedanta's *Health, Safety and Environmental Policy*.

2. SCOPE

This Technical Standard is mandatory and applies to all Vedanta subsidiaries, operations and managed sites, including new acquisitions, corporate offices and research facilities and to all new and existing employees, contractor employees. This Standard is applicable to the entire operation lifecycle (including exploration and planning, evaluation, operation and closure). This standard excludes information security and fraud, bribery and corruption. Operations shall refer to ISO27001 relating to Information Security Management Systems.

3. DEFINITIONS

Definitions of key terms used in this document are shown in the following table.

Term	Definition
Competent Person	An individual who has the necessary and sufficient knowledge, skills and experience, as well as the necessary experience to complete their responsibilities safely, effectively and consistently.
Contractor	Any third party organisation which is engaged or commissioned by Vedanta to undertake work or provide services.
Contractor employee	An employee of a contracted company engaged or commissioned by Vedanta to undertake work or provide services, but who are not directly employed by Vedanta. For example, contractor employees working on Vedanta operations, persons working for Vedanta through staff/employment agencies, contract cleaners etc.
Environmental and Social Management System	The structured framework that provides the arrangements for managing the environmental, health, safety and social aspects through the lifetime of the project.
Environmental Social Impact Assessment (ESIA)	A formalised process designed to identify, assess and document environmental and social impacts associated with a project, along with the mitigation measures and management arrangements for ensuring such measures are implemented.
ICMM (International Council on Mining and Metals)	The International Council on Mining and Metals (ICMM) was established in 2001 and seeks to drive performance improvement through its members which comprise 20 mining and metals companies, as well as 30 national and regional mining associations and global commodity associations.
IFC (International Finance Corporation)	Member of the World Bank that finances and provides advice to private sector ventures and projects in developing countries.

Term	Definition
Operation(s)	A location or activity that is operated by a Vedanta Company and is part of the Vedanta Group. Locations could include mines, refineries, ports or transportation activities, wind farms, oil and gas development sites, offices including corporate head offices, and research and development facilities.
Stakeholder	Persons or groups that are directly or indirectly affected by a project as well as those that may have interests in a project and/or the ability to influence its outcome, either positively or negatively. This can refer to shareholders, lenders, employees, communities, industry, governments and interested third parties.
Stakeholder Engagement	An umbrella term encompassing a range of activities and interactions between Vedanta and its stakeholders over the life of a project that are designated to promote transparent, accountable, positive, and mutually-beneficial working relationships. Stakeholder engagement includes stakeholder identification and analysis, information disclosure, problem/conflict anticipation and prevention, ongoing consultation, formation of partnerships, construction of grievance resolution mechanisms, negotiated problem solving, employee involvement in project monitoring, regular reporting forums and procedures, and other related management activities.
Vedanta Company	A subsidiary of Vedanta Group either fully or majority owned that has its own management structure (e.g. Hindustan Zinc Limited, Vedanta Aluminium Limited, Sterlite Industries limited, etc.)
Security Plan	A document that describes the Project or Operation's plan to address security issues and related events including control measures and response measures for security threats. See also Vedanta Integrated Physical Security Plan.

4. PROGRAMME REQUIREMENTS

This Standard aims to define the minimum processes that need to be established to manage sustainability risks associated with the security of Vedanta's personnel, products and property. The sustainability risks associated with security will depend on the nature of personnel activities, the type of operation and its location. The requirements described below shall be followed by all Vedanta subsidiary companies and operations with regards to the management of security.

4.1. General Requirements

a) Vedanta Group and operations shall ensure that the requirements of this Technical Standard are adhered to as part of the security of their operations to ensure that environmental, social, safety and health impacts are systematically considered in the effective management of security risks.

b) Security management shall also meet the requirements of the *IFC Performance Standards.* These requirements are summarised as follows*:*

- Performance Standard 4 – Community Health, Safety and Security. Vedanta will ensure that the safeguarding of personnel and property is carried out consistently with relevant human rights principles and in a manner that avoids or minimizes risks to the Affected Communities. Security will be provided in a manner that does not jeopardize the community's safety and security, or the Vedanta's relationship with the community and it will be consistent with national requirements, including national laws implementing host country obligations under international law, and the requirements of Performance Standard 4 which are consistent with good international practice.

4.2. Security Risk Assessment

a) Operations shall ensure that a security risk assessment process is in place to identify potential security risks to the operations personnel and property.

b) The process shall include identification of the location specific 'security threat' scenarios that could impact on the operation and the identification of the likelihood and significance of the risks that could result from the threats. Operations shall ensure that the security risk assessment is documented.

c) The security risk assessment shall identify 'High', 'Medium', 'Low' and 'Insignificant' security risks to the operations. Operations shall establish and specify in the risk assessment whether the risks have been accepted, transferred, or will be controlled and/or mitigated.

d) Key security threats that shall be included in the security risk assessment, but not limited to, are:

- Terrorism;
- Organised crime;
- Community unrest;
- Political risk;
- Labour unrest;
- Armed robbery;
- Occupation of an operation or project by local community action group;
- Bomb threat;
- Theft from offices and operations;
- Arson;
- Vandalism;
- Attack on personnel;
- Loss of production;
- Kidnap of personnel;
- Suspect packages; and
- Intentional release from a process unit or storage tank.

e) Vedanta operations shall consider security risks associated with the entire range and stages of their operational activities, including personnel, fixed assets and property and products, and materials being transported. The risks and impacts identification process shall also address negative impacts on workers and the surrounding communities.

Examples of Vedanta's range of operations that may be subject to security risks include:

- Buildings (administration offices, corporate offices);
- Equipment (tanks, processing units, control systems, boilers, turbines, heaters, fuel storage, explosives etc.);
- Support systems (utilities, water supply, wastewater treatment plants, sewer systems etc.)
- Transport (loading/unloading facilities, docking areas, vessels, off-site storage areas etc.)
- Cyber systems and information (computer systems, networks, laptops, cell/mobile phones etc.); and
- Travel (travel between operations, to operations, in-country travel and international travel).

f) The process should engage all relevant business functions to ensure a comprehensive and co-coordinated approach is adopted.

g) Security risk assessments shall be performed periodically and when there is a change in layout, change to external facilities and operations, and after drills and inspections where required.

4.3. Security Plan

a) Operations shall develop a baseline security plan to outline the arrangements to address the High and Medium risks identified in the risk assessment.

b) The plan shall define the controls to reduce High and Medium risks to an acceptable level. These shall comprise as appropriate, a mixture of physical controls (e.g. barriers, layout) as well as security monitoring activities (e.g. inspections and security guard control), resources and procedures.

c) The security plan shall define and describe the arrangements for the implementation of Requirements 4.4 to 4.14 of this Standard and shall also meet the requirements as set out in the Vedanta Integrated Physical Security Plan document.

d) The security plan shall be periodically updated to reflect new information and the current security risks and changing situations.

Security arrangements will typically depend in large part on security risks in the operating environment. In many circumstances, a night watchman may be all that is required, together with some basic security awareness training for staff, sign-posting, or well-placed lighting and fences. In more complex operations and higher risk security environments or travel in a high risk country, Vedanta operations may have to directly employ further security personnel or engage private security contractors, or even work directly with public security forces given in some countries private security may not be permitted (Refer to Section 4.14 on Security and the Community.

4.4. Security Administration and Organisation.

a) Vedanta operations shall ensure that a security manager or representative is appointed or nominated to manage security risks at the operation and to promote a security culture within the operation.

b) The operation shall define and identify in the security plan, other personnel with security responsibilities along with a description of their duties. Personnel with security duties shall

include as appropriate, but are not limited to security supervisors, security guards, receptionists that confirm the identification of visitors etc.

c) A local security incident management team shall be appointed to manage security incidents.

4.5. Training and Competency and Awareness

a) Operations shall ensure that those undertaking security duties have the required competencies to perform their role. This shall include pre-employment checks and references and ensuring they hold relevant qualifications in accordance with local and national legislation. Security guards shall be vetted in accordance with BS 7858 or equivalent.

b) Individuals conducting security risk assessments shall be competent; support may be obtained by external providers if required.

c) The security manager/representative and those with other security responsibilities shall be provided with security related training to enable him/her to perform his/her duties competently. This shall include training and guidance on the issuing and use of firearms and ammunition.

d) Specialist training shall be provided to chauffeurs, security guards and other staff who may face specific security risks.

e) Site/office security is included in the induction of all new employees and contractors and training (see Section 4.6 below regarding training).

f) This incident management team shall be trained in managing security incidents.

g) Visitors shall be informed of relevant security requirements upon arrival at the operations.

4.6. Personnel Security

a) Operations shall develop a personnel security programme to include all locations where employees and contractors are exposed to risk including for offices, sites, and for expatriates residences.

b) Access to security advice shall be available to all staff.

c) An employee security awareness programme shall be developed in line with local security threats identified from the security risk assessment as applicable. This shall comprise at a minimum, information on dealing with security risks such as bomb warnings, suspect mail, abusive phone calls, and aggressive visitors, periodic security awareness briefings including cautioning employees not to speak to outsiders concerning operations related security issues and to abide by security procedures.

d) In locations where there is significant personnel security risk, staff shall be given regular briefings and practical security awareness training annually or when the risk increases.

e) For expatriate employees and dependent:

- a pre-employment briefing shall be provided;
- secure accommodation shall be provided commensurate with risk;
- in country security awareness shall be provided and specialist training where a serious and specific threat is identified; and
- Access to 24 hour assistance shall be in place.

Technical Standard – Security Management

4.7. Communication and Consultation

a) The operations shall determine and define what communications are required for implementing the security plan and arrangements and implement accordingly. This shall include but is not limited to:

- Communications between employees in transit and at fixed asset operations (radios/telephone);
- Communication between the operation and off-site responders and support (e.g. emergency services and appropriate agencies);
- Communication between transport and the fixed operations;

b) Vedanta shall communicate and consult on its security arrangements to employees and Stakeholders such as local law enforcement, subject to overriding safety and security needs, and involve workers and surrounding communities in discussions about the security arrangements through the community engagement process described in the Vedanta Technical Standard TS05 on *Stakeholder Engagement*.

4.8. Access Control

a) Vedanta operations shall implement effective access control security measures at all operations which controls access into, within and out of an operation.

b) The level of access control shall be dependent on the criticality of the area. If the operation designates certain areas as high risk or protected, these shall be subject to a higher level of control or restriction. These areas shall be identified on the security plan.

c) Access control shall include as a minimum but not be limited to:

- Sign in access procedures for visitors, employees and contractors;
- Escorting policies and procedures for visitors, contractors and other persons who seek access;
- Physical security measures, such as key fob entry, fencing, barriers, locks, lighting, and intrusion detection as appropriate; and
- Ensuring security of support systems and site services (electrical and gas supplies etc.).

Other control mechanisms that shall be considered for ‘High’ and ‘Medium’ risk operations include.

- Security guards/dogs;
- Requirements for employees, visitors contractors, truck drivers, railroad crews, government officials and others who may seek access to provide a means of identification;
- Screening and searching procedures for vehicles, baggage, hand carried articles; and
- Mail and package screening systems where identified as high risk.

4.9. Security Drills and Exercises

a) Each Vedanta operation shall conduct periodic security drills and exercises across the identified security threat scenarios as identified by the risk assessment. The extent and frequency of the drills shall be documented in the security plan.

b) A follow up process to address actions from drills and exercises shall be in place and follow up actions shall be tracked to completion.

Based on the risk assessment, for example, a specific Vedanta Low risk operation may find that no drills or exercises are warranted, others may find short focused activities that test one portion of the security programme (e.g. vehicle searches by main gate guards); whilst higher risk operations may require full scale roll out or table top exercises involving multiple groups and off-site responders.

4.10. Security Records and Documents

a) A process shall be implemented for maintaining security related records and their prevention from disclosure. Where possible, existing EHS, quality and other record keeping systems shall be used to avoid duplication and overlap. Maintenance of documentation shall be undertaken in accordance with the Vedanta Group Standard MS09 on *Documentation and Records Management*.

4.11. Security Systems and Equipment Maintenance

a) Security equipment shall be subject to an inspection, test and preventative maintenance programmes. This shall include but not be limited to camera systems, lighting, intruder alarms, fencing etc.

4.12. Inspection and Monitoring of Security Measures

a) Operations shall ensure that property and assets are regularly monitored for unauthorised access and this is detailed on the security plan. The frequency and nature of the monitoring shall be appropriate to the nature and location of the operation.

b) Monitoring shall comprise checks and patrols around the property at a minimum whilst for higher risk, more complex operations, a combination of personal monitoring (guards and dogs) and technology (CCTV intrusion detection and surveillance) may be required. Unmanned low risk operations shall be subject to periodic checks for signs of unauthorised access.

c) Issues identified from checks and monitoring should be recorded, action(s) to address the issues identified and closed within a defined timescale.

4.13. Security Incident Procedures

a) Each operation shall define in the security plan what events constitute a security breach, the required action, roles and responsibilities of those involved, who is to be notified and the escalation process involved.

b) The plan should outline the resources and equipment required for an appropriate response and an orderly recovery process.

c) Vedanta operations shall ensure that contingency plans are in place to deal with security incidents. Contingency plans shall cover where relevant, building evacuation, bomb threats, kidnap etc.

d) The plans shall be coordinated with the operations emergency plan and crisis management plan to ensure that decisions involving regional and corporate crisis management team are detailed along with engagement with the media, community and other stakeholders.

e) A procedure shall be implemented for investigation of security breaches and the requirements for investigation of security incidents including identifying areas for improved security or control measures.

f) Security incidents shall be reported by operations in the local reporting system and to Vedanta Group in line with the *Incident Reporting and Investigation* Management Standard MS11.

g) Employees shall be made aware of the requirement to report the presence of unknown personnel, unidentified vehicles, abandoned packages and other suspicious activities.

4.14. Security Audit

a) The operation shall define how the security plan and arrangements are audited. This shall include periodicity, audit team, reporting requirements and follow up.

b) Regular audits shall be undertaken of the security plan to evaluate the effectiveness of arrangements and risk control techniques. Findings from audits shall be actioned and the security plan updated as required.

Operations may wish to use an existing EHS auditing process or develop their own security audit processes.

4.15. Security and the Community

a) Vedanta operations shall provide security arrangements in a manner which does not jeopardise the community's safety and security and Vedanta's relationship with it. To achieve this, security arrangements shall include:

- Investigation process for any allegations of unlawful or abusive acts of Vedanta's security personnel;
- A reasonable process to ensure those providing security are not implicated in past abuses;
- Ensuring operations do not sanction any use of force except when used for preventive and defensive purposes in proportion to the nature and extent of the threat;
- Adequate training in the use of force (and where applicable, firearms), appropriate conduct toward workers and Affected Communities, and require them to act within the applicable law;
- A grievance mechanism to enable communities to express concerns about the security arrangements and acts of security personnel. The grievance mechanism shall meet the requirements of the Vedanta Technical Standard TS4 on *Grievance Mechanisms*;
- Operations shall avoid as far as possible, the need for employees or security contractors to be armed, there are situations where firearms are appropriate. In such circumstances, it is important that clear instructions are given on how firearms and force should be used. Refer to OGP Guidelines on the use of Firearms;
- Operations whose assets are being protected by public security forces shall encourage those forces to behave consistently with the requirements and principles set out above for private security personnel in order to promote and maintain good relations with the community. Operations shall communicate their principles of conduct to public security forces, and express their desire that security be provided in a manner consistent with those standards by personnel with adequate and effective training. Operations shall

request that the government discloses information about the arrangements, subject to overriding safety and security needs.

5. ROLES AND RESPONSIBILITIES

Vedanta Resources, subsidiaries, businesses, operations and sites shall ensure that roles and responsibilities for implementing and complying with this Standard are allocated. Key responsibilities shall be included in job descriptions, procedures and/or other appropriate documentation.

6. COMPLIANCE AND PERFORMANCE

Each Vedanta operation shall ensure it complies with the requirements of this standard. Performance against meeting the requirements of this Standard shall be assessed periodically documented and, where required, reported to Vedanta Group. The assessment of performance shall include setting and reporting on key performance indicators (KPIs) where these have been established at Vedanta Group, Company or local level. The evaluation of performance shall include, as a minimum, confirmation that:

- A security risk assessment process is in place.
- Security plans have been completed and implemented.
- Assigned Vedanta personnel who undertake security roles have the appropriate competency levels.
- Security plans have defined roles and responsibilities for those involved in security management.
- Security requirements are communicated to all employees, visitors and contractors.
- Access control is provided and implemented;
- Security incident contingency plans are in place and drills are undertaken periodically;
- Incidents are investigated and subject to corrective action;
- Inspections and audits of security arrangements are conducted, and any issues identified have been recorded and addressed.
- Community issues related to security arrangements are addressed.

7. SUPPORTING INFORMATION

Reference	Description
ICMM (International Council of Mining and Metals)	The ICMM has produced and published good practice guidance on a range of health, safety, environment and community issues relating to mining. http://www.icmm.com/library
International Finance	The IFC has published Guidance Notes to guide the

Reference	Description
Corporation Performance Standards Guidance Notes	implementation of the full range of performance standards. These are available on the website. The guidance is currently being updated and draft versions (V2) are available however these have not yet been finalised and formally published. http://www.ifc.org/ifcext/sustainability.nsf/Content/PerformanceStandards
Fire Arms and the Use of Force	http://www.ogp.org.uk/pubs/320.pdf.
Vedanta Integrated Physical Security Plan	Vedanta Group document aimed to develop, implement and monitor an effective and tailor made integrated physical security plan with a benchmark for all industrial units of Vedanta.
BS 7858	Baseline Personnel Security Screening

8. REVIEW

This Technical Standard shall be periodically audited and reviewed to determine its accuracy and relevance with regard to legislation, education, training and technological changes. In all other circumstances, it shall be reviewed no later than 12 months since the previous review.

9. RELATED DOCUMENTATION

A summary of the references and supporting documents relevant to this document is provided in the following table.

Doc. Ref.	Document name
	Vedanta Code of Conduct
POL 06	HSE Policy
MS 09	Documentation and Records Management
MS 11	Incident Reporting and Investigation
TS 04	Grievance Mechanisms
TS 05	Stakeholder Engagement