SECURITY MANAGEMENT PLAN

TNCL-SEC-PLN-0001

APPROVALS:

Title	Name	Signature	Date
Author	Dr. Kudra Said		29/6/2024
Chairperson Standard Committee	Akida Waria		29/6/2024
Worker's Representative	Beatha Kisaka		29/06/2024
Training Lead	Joseph Mwita		29th June 2024
Security Lead	Charles Kisuke		29/06/2024
Community Relations Manager	Moses Rusasa		29/06/2024
Engineering Manager	Eng. Sarai Ally		29/06/2024
OHS&S Manager	Dr. Kudra Said		29/6/2024
General Manager	Rebecca Stephen		29/07/24

Table of Contents

LIST OF FIGURES AND TABLES

1. INTRODUCTION

1.1 Purpose of the Security Management Plan

The Tembo Nickel (TNCL) Security Management Plan (SMP) describes how project security will be managed and delivered and is the overarching document for all other project procedures and policies related to security.

The plan is designed to guide the company's actions at the project in protecting against and mitigating risks of a security and human rights nature that could threaten host communities, TNCL employees, facilities, and ability to operate, as well as protecting the reputation of TNCL and the wider group.

The Security Management Plan will:

- Describe security functions, responsibilities, management and delivery.
- Respond to identified risks with a comprehensive and proportionate security strategy.
- Outline systems to be used in TNCL security throughout the lifetime of the project.
- Consider community risks and impacts posed by TNCL security arrangements.
- Ensure compliance with National Legislation, International Best practices, and Human Rights Standards.

The TNCL Security Management Plan is a live document and will be reviewed and updated after any change in the security-related context in which the project operates, with a full review to be completed on an annual basis.

1.2 Scope

This SMP applies to activities that are relevant to security management (e.g. physical security, access control, material control, etc.) during the Project cycle. This SMP applies to all parties working for or on behalf of the Project having activities relating to security.

1.3 Mission of Tembo Nickel Security

'Tembo Nickel is committed to maintaining the security of our operation and the protection of our staff, in a context that protects human rights.'

1.4 Approach to Project Security

A 'four-tiered' approach to project security will be implemented at TNCL, beginning with regional security, and narrowing down to the most vulnerable infrastructure on TNCL sites. Security infrastructure and procedures will become progressively enhanced through each tier.

The Tanzanian Police Force (TPF) are responsible for and focuses on security in the Regional area and within the host communities, ensuring that the quality of project-affected people's security does not deteriorate due to project-induced in-migration. The TPF will also lead community-based policing initiatives in order to build upon existing security structures in the area and improve communication and relationships between public security and project-affected communities.

Private security will be responsible for providing physical protection and security risk management within the project facilities. Private security will not possess lethal weapons on the TNCL project. It will escalate any criminal issues to the TPF for support if unable to practically respond to an increased security threat or incident. All criminal incidents will be escalated to the TPF, and TNCL will cooperate with Tanzanian authorities, providing information and evidence to support legal investigations. The TNCL security strategy and structure are guided by The Voluntary Principles on Security and Human Rights and IFC Performance Standards 1 and 4. These provide the foundation for responsible security practices inside the TNCL project facilities and within the communities where TNCL operates.

2. ABBREVIATIONS AND MEANING

Table 1: Abbreviations and Meaning

ABBREVIATION	MEANING
CBP	Community-Based Policing
CHRAGG	Tanzanian Commission for Human Rights and Good Governance
CR	Community Relations
EP	The Equator Principles
ERP	Emergency Response Plan
ESG	Environmental, Social and Governance
GoT	Government of Tanzania
GRMP	Grievance Resolution Management Policy
HAP	Henderson Asset Protection
HR	Human Rights
ICON	International Code of Conduct
IFC	International Finance Corporation

IRT	Incident Response Team
MoU	Memorandum of Understanding
PAP	Project Affected People
PIIM	Project Induced in Migration
PS1	IFC Performance Standard 1
PS4	IFC Performance Standard 4 Community Health, Safety and Security
RC	Regional Commissioner
RPC	Regional Police Commissioner
SML	Special Mining License
SMP	Security Management Plan
SOPs	Standing Operating Procedures
SRA	Security Risk Assessment
SRMS	Security and Risk Management Strategies
SWG	Security Working Group
TNCL	Tembo Nickel Corporation
TPF	Tanzania Police Force
VPSHR	The Voluntary Principles of Security and Human Rights

3. OVERVIEW SECURITY SITUATION

3.1 Project Setting

The Kabanga Nickel Project, situated in Northwest Tanzania, was acquired by Kabanga Nickel Limited (KNL), formally known as Lifezone Nickel Limited (LZ), in April 2021. Tembo Nickel Corporation Limited (TNCL) is the local operating partnership owned 84% by KNL and 16% by the Government of Tanzania (GoT), and it is this entity that will develop and operate the mine in Ngara and the Hydrometallurgical Refinery in Kahama. To date (Q3 2023), BHP has invested $100 million between Lifezone Metals and KNL, where BHP owns 17% of KNL, representing 14.3% look-through interest at the TNCL project level. Upon completing a Definitive Feasibility Study (DFS) and Initial Assessment (IA) on Kabanga, which are expected in Q3 2024, BHP can increase its stake in KNL further.

According to the ESIA, the project will directly impact three wards, four villages, six sub-villages and 17 settlements within Ngara District.

Table 2: TNCL Project Affected Communities

Affected Communities, Tembo Nickel Project Area				
Sn	**Ward**	**Village**	**Sub Village**	**Settlement**
1	Bukiriro	Nyabihanga	Rubanga	Rubanga
				Kahororo
2	Bugarama	Rwinyana	Nangeli	Kishiko, Nyabyuya, Mursenge
			Nyabihungo	Murukende, Nyabihungo, Murusenge
			Mutobo	Bweranka, Musagara
		Bugarama	Nyakuguma	Kasana, Mukidakokoye, Nyakanazi, Kungomo, Rutimbura
3	Muganza	Mukubu	Nyakafandi	Nyakafandi, Kumugango

The Ngara region in Tanzania is among the least developed areas in the country, grappling with low levels of education and a labour market predominantly characterised by subsistence agriculture. The introduction of a mine of significant scale is poised to bring about transformative shifts not only in the economic landscape but also in the social and political dynamics in the region through Project-Induced Immigration. The Kabanga Nickel Project can potentially reshape the culture of the local population.

The TPF in the region is generally understaffed and poorly equipped, and it has little or no means of communication, transport, or operational budget. The Memorandum of Understanding between Tembo Nickel and the TPF is essential to ensuring that public security can provide adequate law and order in Ngara and project-affected communities as the mining asset is developed. The MoU also ensures a transparent arrangement for support to be provided to the TPF and that VPSHR is prioritised in the local security strategy.

Tanzania is preparing for a general election in 2025. It is undoubtedly the region's most stable country, making significant security impacts arising from civil disobedience or instability near the Kabanga site extremely unlikely.

The site's remote location, less than one kilometre from the Burundi border, places it geographically within the Great Lakes Region, which has historically faced political instability. Although the current situation in Burundi appears calm, historical precedents underscore the potential for escalation in this geopolitical zone. The border area, known for its porosity, remains susceptible to cross-border security incidents, evident in four reported community robberies in Ngara District in Q4 2022. Such incidents can intensify in the local area as the economic and enterprise environment develops.

Regionally, the previous election in Burundi, whilst the most peaceful in its democratic history, was condemned by Amnesty International for political violence and extrajudicial killings in the build-up. The DRC is experiencing an uptick in instability in the Eastern provinces of North and South Kivu near its Rwandan borders. Democratic Republic of Congo, Rwanda and Burundi will have general elections in 2023, 2024 and 2025 respectively. Historically, elections in these states have featured political violence and instability. Whilst low, the most significant risk to the TNCL project from regional events is a surge in migration and asylum-seeking in the Ngara Region. Refugee influxes into North-Western Tanzania may be associated with a worsening crime and community health landscape in affected areas.

Figure 1: TNCL Project Setting

3.2 Security risks

The HAP October 2023 Project Security Risk Assessment identifies the key five risks heading into the early works and construction phase:

1. VPSHR and Use of Force violations by Private and Public security representatives.
2. Theft of fuel, equipment, and materials
3. Speculation and encroachment on company land
4. Mis-managed Project Induced In-Migration
5. Community dissatisfaction leading to unrest

The October 2023 Security Risk Assessment analysis identified that the project's security risk exposure will be closely correlated with the project's risks and impacts on the host community. Current community motivation to enact security threats is low, and the community is generally satisfied with the project's presence. Rising community dissatisfaction should be expected to increase the risk of community unrest and criminal motivation against the project. Protection of the Social Licence to Operate (SLO) will be the central risk management requirement of the Kabanga project.

As mining activities ramp up and equipment and materials arrive at Kabanga locations, opportunistic and organised criminal attempts will rise. Any perceived or identified weakness in security strategy or infrastructure will lead to sustained attempted thefts on targetable assets, from small-scale opportunistic attempts to organised infiltration of TNCL supply chain mechanisms. Notably, as the number of security incidents increases, the risk of VPSHR violations and loss of the SLO will also increase. Considering the focus on ESG in extractive capital markets and Tanzanian political discourse, this escalation must be avoided or may pose existential risks to the project.

Once compensation payments are made, newly acquired land must be quickly secured to avoid speculation and encroachment. Suppose cultivation and settlement are allowed to increase. In that case, there will be delays and grievances as TNCL attempts to remove crops or structures, potentially leading to court cases and claims of illegal evictions.

The beginning of construction will lead to Project Induced in Migration (PIIM). Most new arrivals will be seeking employment with subcontractors or setting up downstream enterprises. This will require careful management to mitigate negative community impacts.

Construction starts will also increase risks to the community. Compensation payments will be a trigger of intra-community crimes, including robbery, theft, and violence against vulnerable groups as 'jealous neighbour syndrome' takes hold. Social ills such as prostitution, drug abuse and alcoholism will also fuel rising crime rates. Empowerment of public security forces through the Memorandum of Understanding with the Police and Security Working Group (SWG) will be central to managing these risks.

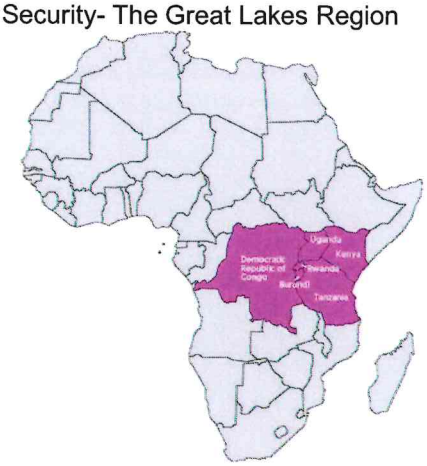
4. PROJECT SECURITY STRATEGY

The Security Risk Assessment forms the basis of the Security Management Plan (SMP), with International Finance Corporation (IFC) Performance Standards and the VPSHR as the guiding principles. The SMP will evolve as the mine matures through the different phases of development and will stipulate the required security services, resources, procedures, and protocols needed to manage the security situation.

The TNCL project security strategy is based on four tiers, with each concentric ring of security becoming progressively more secure in terms the closer one gets to the TNCL critical assets:

1. **Regional Security** - Threats from the Great Lakes region.
2. **Security of the local area** - The project affected communities, including the Burundi border.
3. **Security of the Tembo Nickel Project** - The Project Area.
4. **Security of TNCL key assets** – Staff, critical infrastructure, land, IT systems, and construction equipment.

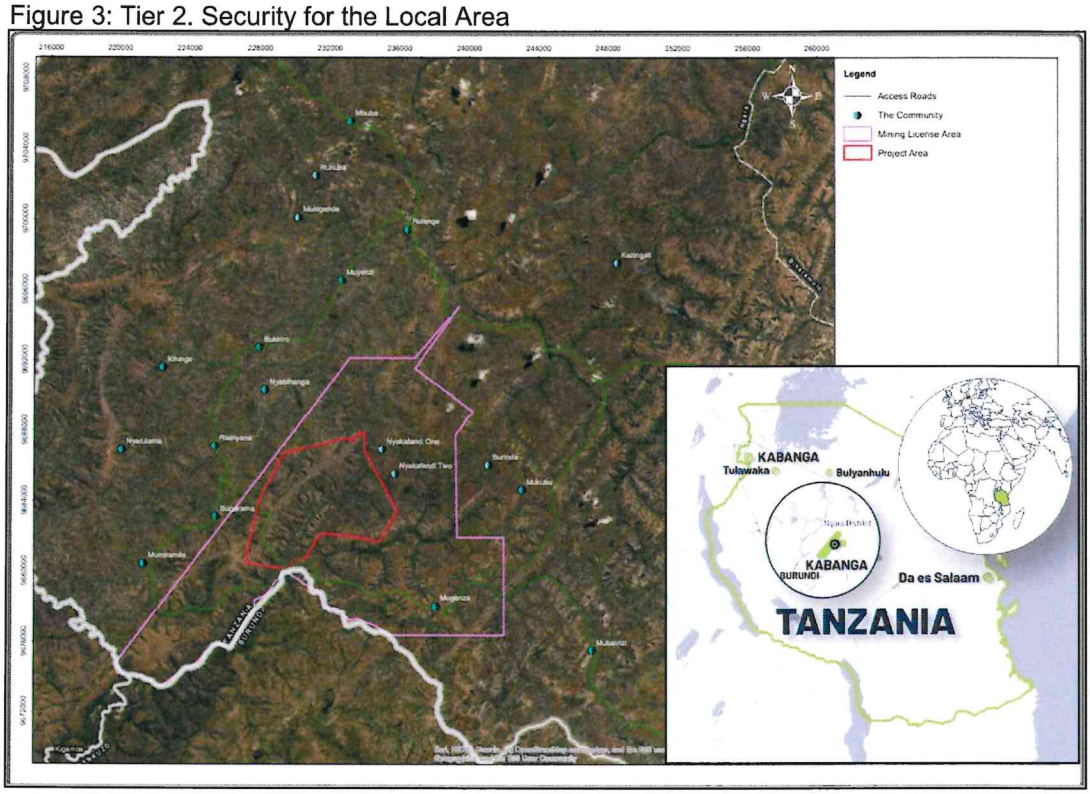
Figure 2: Tier 1. Regional Security- The Great Lakes Region



The geographical location of the Kabanga Nickel Project lies almost central to the African Great Lakes Region. Therefore, the project can be influenced by this Region's political, social and economic situation. Primary responsibility for regional security remains with public security and is governed by the Regional Security Committee, chaired by the Regional Commissioner in Bukoba. As in most remote areas of Tanzania, the TPF are understaffed and poorly equipped, with little means of communication, transport, or operational budget to improve their effectiveness. The TPF in Ngara District faces the same challenges. Tembo Nickel is expected to assist financially in improving their operational capability, details of which are articulated within the MoU agreement signed on 12 May 2023. At the District level, the same governance format exists, and the local public security falls under the responsibility of the District Security Committee chaired by Ngara District Commissioner Colonel Matthius Kahabi, a vital member of the TNCL Security Working Group.

Key to managing this regional security tier is the Tembo Nickel Security Working Group, through building good working relationships with the Regional and District levels of the Government of Tanzania. Positive communication and relationships will allow for proactive information sharing to assist in the early identification of threats with the potential to affect the Kagera Region, Ngara District, and the Kabanga Nickel Project. A robust but flexible MoU agreement with the Tanzanian Police Force has been established to ensure that the level of support provided to the project by the police can be amended on a risk-based approach. Therefore, should the SWG identify an increased period of risk, increased public security support can be requested for a defined period to manage regional risks.

Figure 3: Tier 2. Security for the Local Area



The October 2023 TNCL Project Security Risk Assessment found that the project's security risk exposure will be closely correlated with the risks and impacts of the project to the host community, and community dissatisfaction/unrest is a top 5 risk to the project and its successful progression. Whilst, as of December 2023, the community are generally satisfied with the project's presence, rising community dissatisfaction should be expected as the project progresses. The key to managing the local security risks and maintaining the social licence to operate (SLO) is a security strategy underpinned by IFC Performance Standard 4 and the Voluntary Principles on Security and Human Rights.

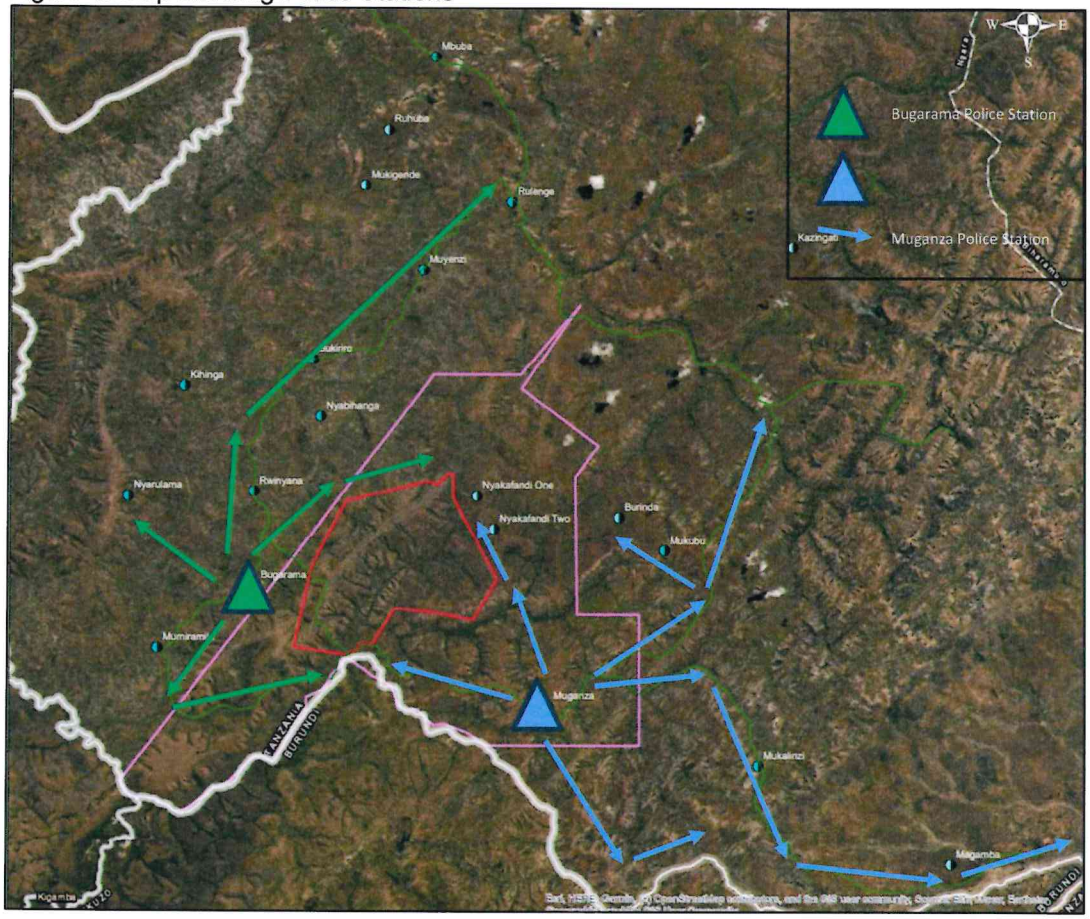
The beginning of construction will lead to Project-Induced In-Migration (PIIM). While this may ultimately benefit trade, employment, infrastructure and services in the local area, in-migration can also negatively affect host communities, specifically regarding community health, safety, and security. These negative impacts can result in increased operational and reputational risk if not managed, ultimately jeopardising TNCL's SLO. TNCL can only be as secure as the local community allows. Hence, assessing the risks that the local community faces from the project and developing ways to manage these risks are critical parts of the security strategy proposed

by HAP. Without the management of PIIM, case studies have shown an increase in criminality whilst a simultaneous decrease in local law and order capability due to the sharp rise in population and police workload.

In this local area, Public Security organs are responsible for policing, responding to and investigating all criminal activity, controlling demonstrations or civil disorder, and all other responsibilities of public authorities. Providing additional public security services that utilise best practices and are delivered responsibly will improve community security and support the maintenance of the project's SLO. Due to the current gaps in policing capability in the project-affected communities, the key to effective and responsible security within the local area is the MoU agreement between TNCL and the TPF.

The long-term goal of the MoU is to empower the TPF to protect law and order for a rising population in host communities whilst operating in a manner that glorifies Human Rights consistent with IFC PS4. Based on current risk assessments by HAP, the TPF within Ngara District could not cope with the additional strain caused by the influx and the associated rise in expected criminal activity without further support from the project. A long-term TPF support plan, documented within the MoU, will include the rehabilitation of Bugarama Police Station to a Class B police station capable of housing 50 – 100 police officers. A new Class C police station will also be constructed in Muganza and can accommodate up to 50 police officers.

Figure 4: Map showing Police Stations

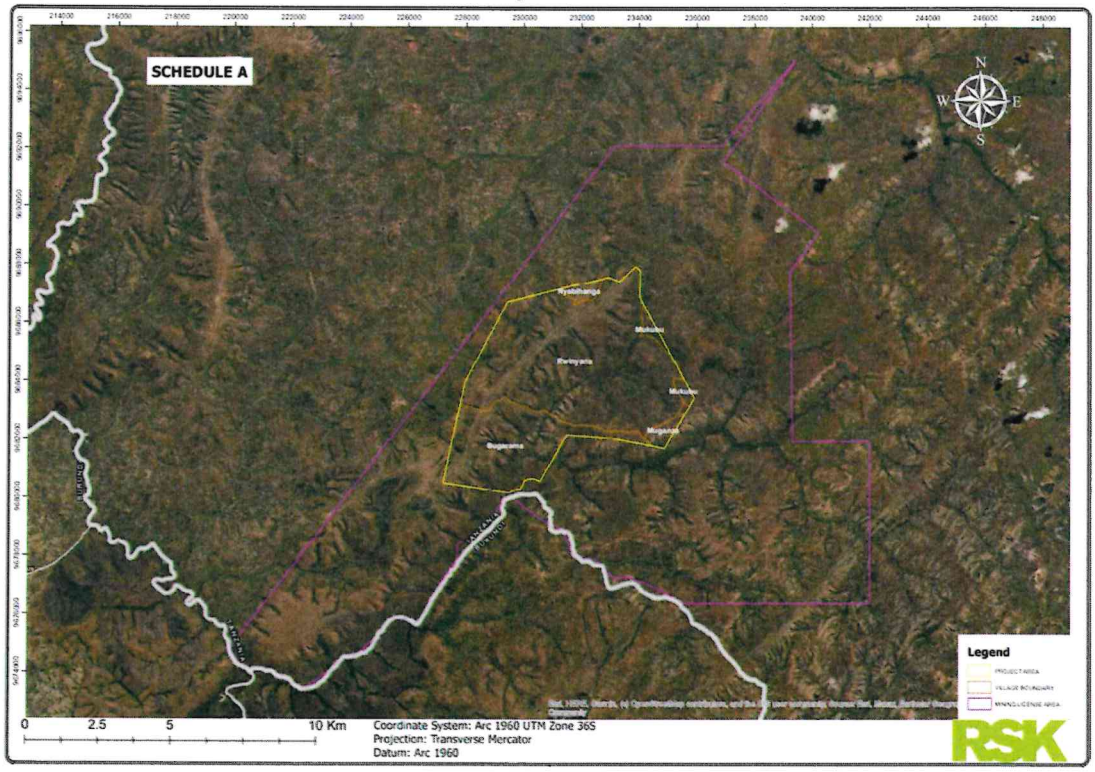


As shown in the above diagram, two police stations on opposing sides of the project will provide not only improved community security but also multiple project benefits, including 'all-round defence', cut-off points for security incident support, and more excellent monitoring and response capability of the project southern access road and paralleling Burundi border. Through the MoU, logistical support for additional police workforce in the area will be provided by TNCL by a patrol vehicle, which will enhance patrol capability and improve response times to security incidents within communities and projects where required. Currently, at 300L per vehicle per month, a pre-designated amount of fuel is allocated within the MoU to support police patrols and incident response.

In addition to the increased police presence in the area, The Tanzania People's Defence Force (TPDF) has a military outpost 8km from the project site and is assigned to maintain the security of the Tanzanian borders in the Region. The TPDF will support security for the local area by responding to serious border issues or incidents that require an escalation from the local police's capability.

Quarterly neighbourhood security engagement meetings involving critical Burundian security organs from the Muyinga and Cankuzo Regions have also been established. The intention of the meetings, similar to the Security Working Group, is to build relationships between security actors along the border area to improve communications, identify threats to the area before incidents occur, and joint incident response and investigation for cross-border issues where criminals may flee across the border to avoid detection. Key precisely to the TNCL project will be an early warning of an adverse change in atmospherics towards Tanzania and the project with the potential to escalate into cross-border dissatisfaction and unrest.

Figure 5: Security for the Tembo Nickel Project Area



Schedule A- The TNCL SML and Project Area

The third tier of the security plan focuses on the TNCL Special Mining License (SML) area, specifically within the initial Project Area. Here, the emphasis switches from public security policing to private security safeguarding. The role of private security is distinctly separate from that of public security, and the remit is asset protection and access control, which are solely within the project area. Should an identified risk or serious security incident occur which is beyond the capability of the private security, TNCL may request through the Site General Manager TPF support to control the risk or respond to the incident, similar to any other community member requiring public security support.

Around the Project Area, the outer barrier demarcation will appear non-threatening to blend as much as possible into the local environment. Still, it will provide sufficient protection against accidental intrusion by humans or animals. Critically, it will not be effective against determined intruders. As per the original plans for the Ngara site, a 20 m cleared safety zone would be established in the immediate vicinity, and an 80m buffer zone, where cultivating and grazing are not permitted. To complement the demarcation boundary, the project area will be monitored by technology and patrolled, and threats will be responded to by mobile units as described in detail below. Basic but scalable technical security installations, including Long Range PTZ CCTV cameras, drone patrols, and security-focused lighting, will be established early during construction and then upgraded as the project develops. Such capabilities will be managed from a security control room to support the physical security units on the ground.

Figure 6: Project Area Security Plan

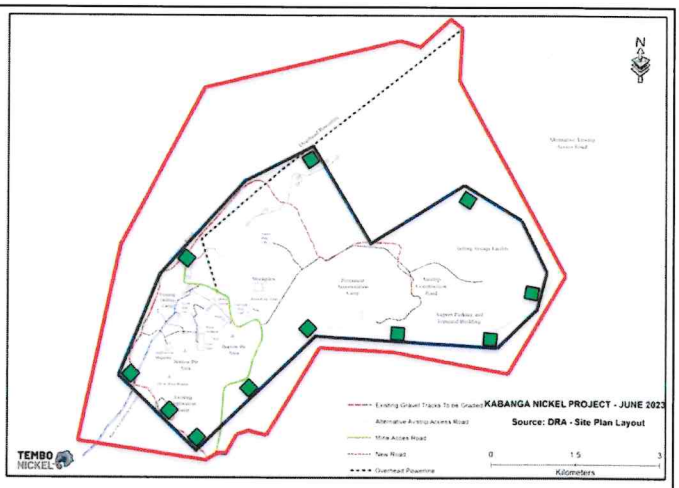
Project Area Boundary to be demarcated by concrete beacons as part of RAP following relocation of PAPs

Green fence plus medium fence to provide project area barrier (27km).

Medium security fence around security perimeter (Crime Prevention Through Environmental Design using natural high features).

CCTV (Video Motion Detecting) with interlocking arcs (LOS) providing surveillance and movement detection within the project area- priority to South overwatching Burundi approach routes.

Drone Technology to provide outer perimeter patrols and intruder



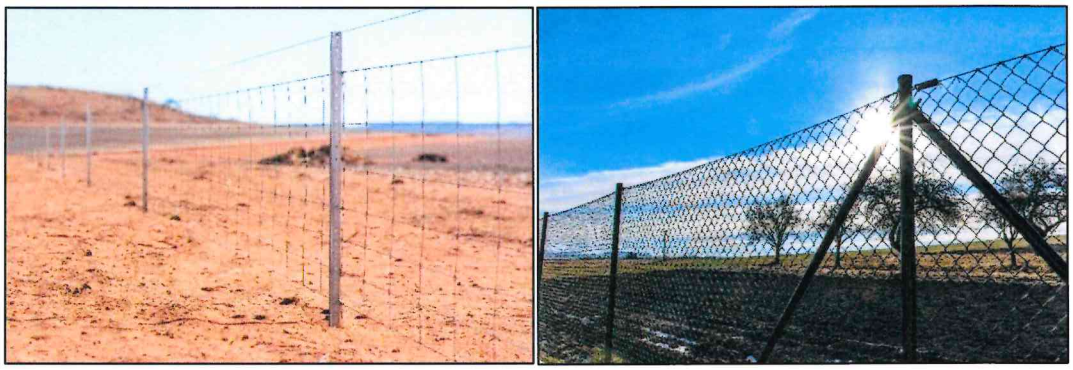
A combination of a natural barrier (TBD) and fencing is still envisaged. An 80m buffer zone will be cleared between the natural barrier and the fence, and no farming or cultivation will be allowed within the buffer zone. An additional 20m cleared zone will serve as a fire break outside the fence, and a 7m access track inside the wall will be established for security patrols. The general security fencing philosophy includes positioning security fences and CCTV cameras on natural high features to maximise line of site and surveillance capabilities. Concrete poles and stay posts should be considered for fencing as they offer a lower theft risk.

Fencing

The type of fence will be determined by the specific needs of the project including the desired level of security, budget constraints and maintenance requirements. The following fencing standards have been identified for each level of security fence, ranging from Low security to high security.

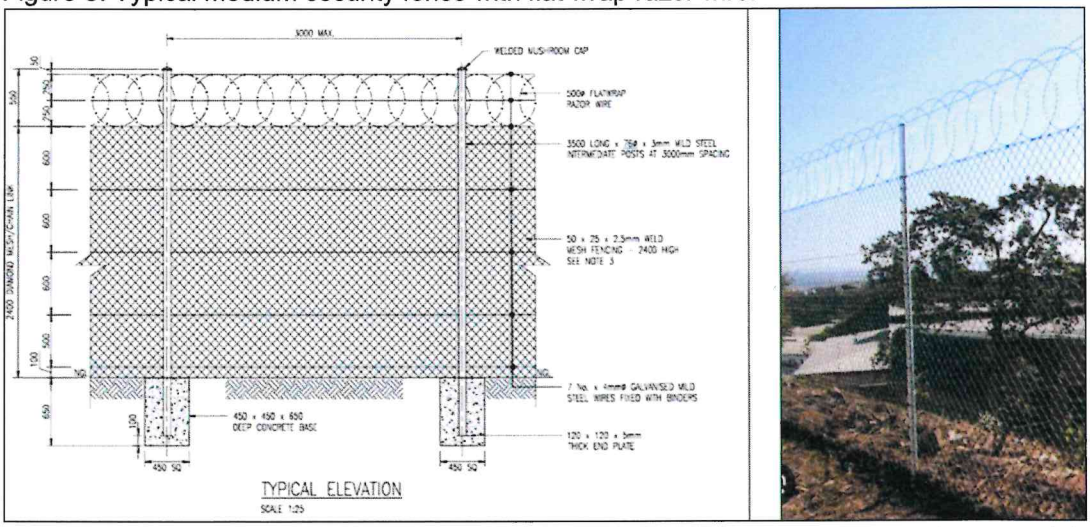
- **Standard (Low Security) fencing** which is intended primarily as a safety barrier to prevent people and animals from inadvertently entering the project area and deter intrusion against all but determined intruders.

Figure 7: Typical Standard Security Fences



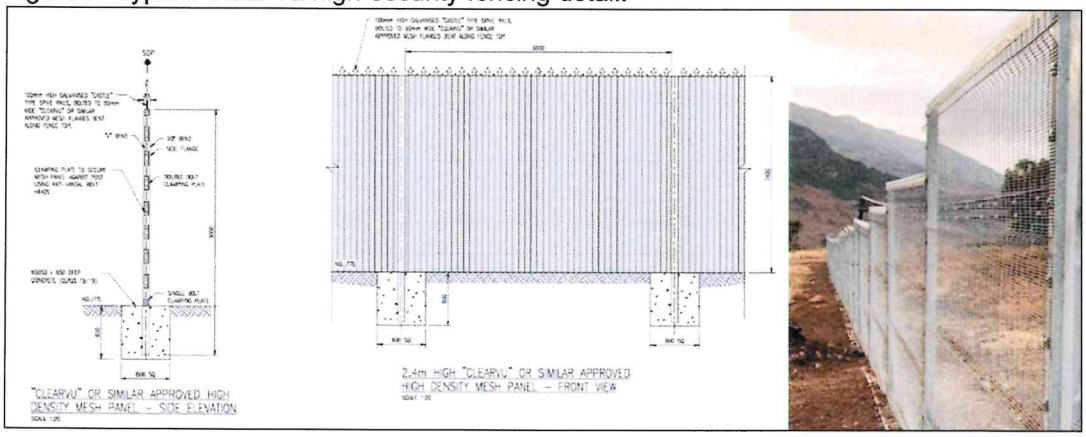
- **Medium Security fencing** - primary function is to deter intrusion into restricted areas of the project site to prevent unauthorised access to the property and the mine's material, equipment, and other assets.

Figure 8: Typical medium security fence with flat wrap razor wire.



- **High-security fencing** - to deter determined intrusion into areas where a risk assessment has indicated that there is a requirement for a higher specification barrier. This requirement may arise due to the high-value nature of the assets to be protected or the dangerous nature of substance storage in the area. High-security barriers are installed to limit the risk of harm to personnel from outside intrusion.

Figure 9: Typical Clear-vu high-security fencing detail.



Surveillance of the project perimeter will be monitored through a mixture of environmental design, technological systems and manned security patrols.

Environmental design can utilise a combination of measures including how you design a space and position assets, processes, and activities within it to design out criminal behaviour is known as Crime Prevention Through Environmental Design. For example, as shown in Figure 9, by intentionally placing fencing on naturally high features, a wider area of coverage can be covered by co-located CCTV cameras, deterring less motivated adversaries from attempting intrusion into the project area, whilst increasing the chance of detection of intrusion by those more determined criminals. Critically, this approach reduces necessary budgets for expensive security technology.

Surveillance of the project perimeter will be monitored through a mixture of environmental design, technological systems, and manned security patrols.

Environmental design can utilize a combination of measures including how you design a space and position assets, processes, and activities within it to design out criminal behaviour is known as Crime Prevention Through Environmental Design. By intentionally placing fencing on naturally high features, a wider area of coverage can be covered by co-located CCTV cameras, deterring less motivated adversaries from attempting intrusion into the project area, whilst increasing the chance of detection of intrusion by those more determined criminals. Critically, this approach reduces necessary budgets for expensive security technology.

CPTED is based on several principles:

1) **Natural Surveillance.** Increasing the eyes on a targeted asset or building. A premise being overlooked was ranked the second most powerful deterrent for British burglars, behind security guards present, in a 1994 study.
2) **Natural access control**. This entails the use of structures, barriers, signage, landscaping and lighting to clearly delineate the ownership of a space and guide movement through a space. This enables easy identification of suspicious activity for authorised users and restricts unauthorised entry – for example by placing thorny bushes below unsecured windows or restricting exterior access to roofing.
3) **Natural territorial reinforcement**. This involves creating a sense of ownership over a space by authorised users. A sense of 'owned' space makes individuals more likely to challenge those they perceive to be unauthorised, a powerful detector and disruptor of criminal incidents as it turns all your staff into security guards. This is closely related to natural access control through its use of landscaping, signage and lighting. Simple measures such as keeping spaces neat and tidy, mandating the open wearing of ID cards and awareness programmes empowering staff to buy into security goals will go a long way to empowering individuals.
4) **Management and maintenance**. Quite simply, people are more likely to take ownership of a space if they feel proud of it. It is important that lighting, paint, signage, fencing, walkways, windows, and doors are kept in good order.
5) **Compartmentalization**. Just as the spread of a fire can be slowed by increasing the number of internal doors, the job of an adversary can be made more difficult by providing layers of access control. Layers of delays allow more time for detection and disruption of an adversary.

When CPTED is combined with other measures such as CCTV and policy and procedures, this is known as Situational Crime Prevention (SCP). The purpose of SCP is to build security measures onto a well-designed space to further deter adversaries. It achieves this by drawing on the Rational Choice Theory of criminal motivation to shift the perceived risk and reward of an offence in favour of the enterprise. This is outlined in the figures below:

Figure 10: SCP principles for shifting the risk/reward balance of crime in favour of the enterprise.

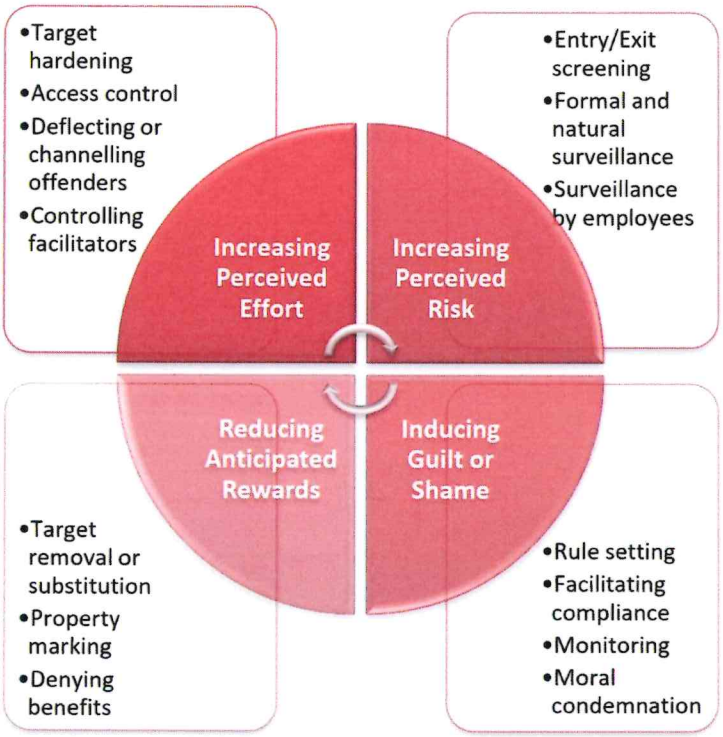


Table 3: 25 SCP approaches

Increase the Effort		Increase the Risk		Reduce the Rewards		Reduce Provocations		Remove Excuses	
1	Target Harden *robbery glazing*	6	Extend Guardians *neighbourhood watch*	11	Conceal Targets *remove branding on trucks*	16	Reduce Frustrations *polite guarding service*	21	Set Rules *circulate ethical expectations*
2	Control Access to Facilities *card access*	7	Assist Surveillance *lighting*	12	Remove Targets *disable computer USB ports*	17	Avoid Disputes *engage community proactively*	22	Post Instructions *notice listing prohibited items*
3	Screen Exits *electronic article surveillance*	8	Reduce Anonymity *visibly displayed badges*	13	Identify Property *property marking*	18	Reduce Emotional Arousal *ban discrimination*	23	Alert Conscience *solar LED speed display signs*
4	Deflect Offenders *limit site entry points*	9	Utilise Place Managers *reward vigilance*	14	Disrupt Markets *anti-illicit trade initiatives*	19	Neutralise Negative Peer Pressure *engage & defuse*	24	Assist Compliance *employee assistance*
5	Control Crime Facilitators *secure vehicles*	10	Strengthen Formal Surveillance *guards*	15	Deny Benefits *remote disabling of stolen laptops*	20	Discourage Imitation *rapid maintenance*	25	Assist Reporting *anonymous hotline*

Drone technology will be utilised to deliver an effective airborne surveillance system around the project area perimeter, whilst also providing a quick reaction surveillance tool to support the ground team's response during a security incident.

Other capabilities will include:

- Semi-autonomous waypoint navigation.
- System can be landed, recharged with replaceable batteries, and re-used.
- System can employ a range of payloads (CS and criminal marking paint).
- System is augmented with night vision capability.
- Flight times of 45+ mins which can be enhanced depending on payload.
- Live time monitoring by operator and Security Control Room.
- Low acoustic signature for covert surveillance.
- Tethering capability for permanent aerial surveillance of key areas.

Drone surveillance and monitoring will reduce the requirement for large manned guarding teams and mobile patrols, whilst supporting other TNCL strategies including decarbonisation through a reduction of patrol vehicles.

Response

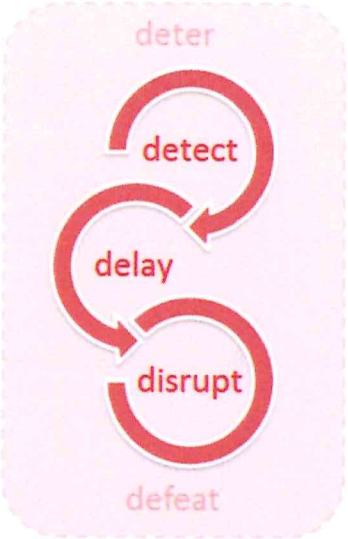
Response teams are essential to an effective surveillance program to provide a quick response in reaction to the detection of criminal activity. Fully manned Private Security Mobile Response vehicles will be stationed at strategic points within the project area to support surveillance teams.

5. SECURITY FOR TEMBO NICKEL KEY ASSETS

The fourth tier consists of strong procedural, human, physical and technical security mitigations to protect the project's most sensitive assets such as accommodation compounds, processing plants, explosive magazines, and fuel depots. The project security risk assessment notes that the most likely risk to be faced by the project is systematic theft based on collusion.

The project mitigation strategy is based on the Five Ds. These are Deter, Detect, Delay, Disrupt, and Defeat, as outlined in the figure below.

Figure 11: The 5 D's.



1) **Deterrence**: Deterrence is achieved by implementing measures that are perceived by potential adversaries as undesirable to attempt to defeat (cost, time, difficulty, surveillability etc.). Deterrence can be very helpful in discouraging attacks by casual adversaries, who may be displaced onto a less well-protected target. However, deterrence is ineffective against a determined adversary who is set on specifically attacking you. Deterrence is closely related to SCP principles.
2) **Detection:** Security systems should be designed to detect adversaries attempting to carry out an offence. From a cost and business interruption perspective, detection is better when it takes place before an undesirable event rather than after. The emphasis in corporate security is first and foremost to try to prevent the undesirable event. Catching the adversary red-handed is secondary. The best system is that which provides the earliest detection, and strong delays can significantly assist in assuring that detection takes place, and that there is sufficient time to detect it effectively. Early detection at the site perimeter increases the available response force time after detection. Detection should aim to not just identify the presence of an adversary but to also provide information to assist the response capacity.
3) **Delays:** Delays provide time for detection to take place. The terms delay and barriers are often used interchangeably but are not synonyms as the latter may sometimes infer an ability to prevent an adversary action.
4) **Disruption:** Disruption is a measure of the effectiveness of response in neutralising the adversary and ideally preventing the undesirable event. For effective interdiction, the information communicated to the response force should include details of the strength, nature and sophistication of the adversary, weapons, direction of travel and an indication of the intended adversary action and target. In the case of a perimeter intrusion, for example, accurate assessment allows for the response to:
    - Arrive at the correct location.
    - Arrive in the correct strength.
    - Arrive within a defined timeframe, which should be less than the minimum delay value of the barrier.
5) **Defeat:** Defeat builds on disruption to effectively apprehend an adversary if an attack has been carried out and recover losses to the extent possible.

5.1 Access Control

Access into the TNCL perimeter and working areas will be controlled. Standard Operating Procedures have been developed and approved for personnel, visitors, and vehicles entering TNCL facilities which are enforced by the contracted private security provider. All staff movement in/out of the site will be accompanied by a management-approved offsite movement pass, and all visits to TNCL facilities will be pre-approved by TNCL management 72 hours in advance through a Visitor Request Form. As the project moves into the construction phase automated and biometric access control installations will be designed and implemented to provide additional levels of security at key assets within the project area. TNCL-SOP-SEC-0001 Access and Material Control explains in detail the current and approved access control procedures.

5.2 Asset Protection

A TNCL material gate pass is required to accompany any company items leaving the Kabanga site or Drill Camp. Failure to produce a valid TNCL gate pass, signed by an approved authorized person, will result in the security officers not allowing egress off the TNCL site. TNCL-SOP-SEC-0001 Access and Material Control explains in detail the TNCL asset protection procedures. Company-issued and personal electronic items must be registered on the TNCL Staff Asset Declaration Form for record of entering the site and authorisation to remove from the site. This form will be approved by department managers/leads and be also signed by the Security Control Room. A copy of the Declaration Form will be required to be shown to the security officers at the main gate to allow the item to be removed from the site.

5.3 Security Searching to support Access Control and Asset Protection

All vehicles entering or exiting TNCL sites may be requested to go through vehicle and baggage searching by the security team. Searches will be completed at random using a lottery method. Should a driver be selected for search through this method then the vehicle will be instructed to move to the vehicle searching area for a systematic search of vehicles and baggage. All searches will be recorded on the HAP vehicle search log with records stored in the security control room. Refusal from any driver or person to allow search will result in the vehicle being denied access/egress from TNCL sites and will be escalated to the senior security personnel on site for further instruction. TNCL-SOP-SEC-0001 Access and Material Control explains in detail the current and approved searching procedures.

5.4 Security Fence Type by Location

Within the project area, different locations have been assessed to understand the fencing requirement. A summary can be found in the below table of fencing specifications at each location within the project area ranging from electrified high-security fences at accommodation areas and explosives magazine, to standard security fencing at contractor laydown areas.

Table 4: fencing specifications

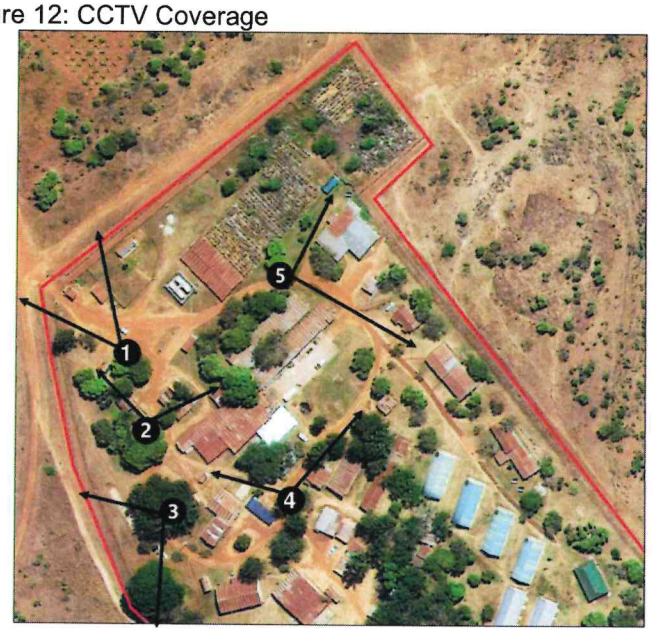
Security Zone	Fence type and height	Flat wrap razor wire (Y/N)	Access track for patrols (Y/N)	Fire Break (Y/N)
Overall site perimeter	Outer green fence with buffer zone and inner standard security diamond mesh fencing -1.8m high	Y	Y	Y
North Box cut Area	Medium security diamond mesh fence with flat wrap razor wire -2.4m high	Y	Y	Y
Conveyor Box cut Area	Medium security diamond mesh fence -1.8m high	N	Y	Y
Tembo Box cut Area	Medium security diamond mesh fence -1.8m high	N	Y	Y
Concentrator Plant and Mine infrastructure area.	Medium security diamond mesh fence -1.8m high	N	Y	Y
Tailings Storage Facility	Medium security diamond mesh fence -1.8m high	N	Y	Y
Landfill site	Medium security diamond mesh fence -1.8m high	N	Y	Y
Aerodrome	Medium security diamond mesh fence -1.8m high	N	Y	Y
Explosives Storage Magazine	Electrified medium security diamond mesh fence with flat wrap razor wire -2.4m high	Y	Y	Y
Drilling Camp (Major Camp)	Electrified medium security diamond mesh fence -2.4m high	N	Y	Y
Exploration Camp	High security electrical outer perimeter fence with a medium security inner fence as per current standard -2.4m high	N	Y	N
Permanent Accommodation Camp-	High security electrified Clear-vu fence-2.4m high	Y	Y	Y
Contractors' laydown areas	Standard security diamond mesh fencing -1.2m high	N	N	N
Cable yards, storage yards, salvage	High-security Clear-vu fence-	N	Y	Y

Security Zone	Fence type and height	Flat wrap razor wire (Y/N)	Access track for patrols (Y/N)	Fire Break (Y/N)
yards	2.4m high			
Hazardous storage areas	High-security Clear-vu fence-2.4m high	N	Y	Y
Quarries and borrow pit areas	Medium security diamond mesh fence -1.8m high	N	Y	Y
PCD's	Standard security diamond mesh fencing -1.2m high	N	N	N
Overland conveyors and pipeline servitudes	Standard security diamond mesh fencing -1.2m high	N	Y	N
Vent Fan Stations	Medium security diamond mesh fence -1.8m high	N	Y	Y

5.5 CCTV

A comprehensive CCTV plan will cover the key assets, monitored by the security control room for intrusion detection, and response, and to provide video evidence of incidents that can be used to support criminal prosecutions. At present for phase 1, five CISCO CCTV cameras have been purchased for the Kabanga Site, with planning ongoing for CCTV monitoring systems on the wider Kabanga Nickel Project. CCTV system will be connected and transfer data to a CCTV control room where the database and monitoring screen are installed. CCTV recordings shall be kept at least for 30 days. An alternate electrical power system shall be installed to ensure the uninterrupted operation of electronic security systems in the event of a power outage.

Figure 12: CCTV Coverage



1. Site Main Gate Camera
CISCO Meraki MV52 pole-mounted bullet camera with 37° field of view 4k day/night subject identification and licence plate recognition camera.

2. Fuel Pump and Fuel Station Camera
CISCO Meraki MV93 structure-mounted (generator housing). Fisheye camera 180° field of view motion indexing 2880x2880 HD day/night video resolution.

3. Workshop and Stores
CISCO Meraki MV93 pole-mounted (generator housing). Fisheye camera 180° field of view motion indexing 2880x2880 HD day/night video resolution.

4. Car Parking Area
CISCO Meraki MV93 pole-mounted (generator housing). Fisheye camera 180° field of view motion indexing 2880x2880 HD day/night video resolution.

5. Clinic and Mess
CISCO Meraki MV93 pole-mounted (generator housing). Fisheye camera 180° field of view motion indexing 2880x2880 HD day/night video resolution.

5.6 Security Control Room

The TNCL Security Control Room (SCR) acts as the nucleus of the TNCL Security Operation monitoring and reporting on all aspects of TNCL security. Control Room Operators are responsible for processing alerts of breaches of the physical security barriers through the technical security systems available, and information received through staff and security officers. The Security Control Room will coordinate an initial security response to an incident through mobile response units, as well as alerting the security management team of the incident. The following responsibilities are currently carried out within the TNCL SCR.

5.7 Emergency Call-Out Procedure

The Emergency Callout Procedure instructs all emergencies to be reported through the Security Control Room. This ensures that a trained operator answers the call, with knowledge and contact information of the correct persons that are required to be notified for each type of incident, and therefore the quickest and most effective response possible. Emergencies can be reported through VHF radio Emergency Channel 4, or through the TNCL Security Control Room emergency phone number, which is communicated regularly to TNCL staff. The full Emergency Call-Out Procedure can be found at TNCL-OHS-SOP-0033.

5.8 Key Control

TNCL utilises a strict key control system at sites to ensure that the security of facilities and offices is maintained. TNCL-SOP-SEC-0002 Key Control Procedure explains in detail the current and approved key issuing, returning, duplicating, and lost key procedures.

5.9 Vehicle Satellite Tracking

As part of TNCL journey Management operations, TNCL and contractor vehicles are fitted with satellite tracking devices which are monitored from the Security Control Room. SCR operators are responsible for ensuring that all devices are active and being monitored 24 hours a day. Any vehicle deviating from expected routes or approved vehicle movement timings, over speeding, are identified by the SCR with the information escalated to the site security manager for action. Following an LV incident, SCR operators will provide vehicle locations to response teams, and movement reports to assist with post-incident investigation.

5.10 Accommodation and Office Panic Alarms

As of December 2023, 191 accommodation and office panic alarms are fitted at the Kabanga Site, which can be activated in the event of an emergency to quickly notify the SCR. On receiving a panic alarm, the SCR will coordinate an immediate response through HAP mobile response or shift commanders. The responding commander will provide initial feedback of findings to the SCR who can then coordinate the appropriate escalation and emergency response to the situation.

5.11 Electric Fence Operations

TNCL Kabanga Site and Drilling camp are protected by Gallagher-style electric fencing, comprising of 6 and 2 zones respectively. Once an electric fence activation occurs, the SCR operator receives the notification within the SCR and will coordinate the initial investigation into the alarm through an available HAP commander. On arrival, the commander will report back to the SCR with findings, with the operator able to then escalate the situation and coordinate the appropriate response as required. All unplanned alarms for SCR systems are logged within the HAP Unplanned Alarm Log for data metric reporting purposes.

5.12 VHF Radio Operations

TNCL Operates a VHF Radio communication System for on and offsite staff to the Security Control Room. The security and emergency channels are monitored 24 hours per day by the SCR. Should an emergency call be received on the emergency channel, TNCL-SOP-

OHS-0033, Emergency Call-Out Procedure will be initiated by the SCR Operator. Hourly post checks are also completed at all security posts to confirm the welfare of security staff. Should a post not respond an investigation will commence until communication has been established. Any unusual activity reported through VHF radio channels will be logged and escalated through the security chain of command.

5.13 Emergency Siren Notification

The Kabanga Site Emergency Siren is located with the SCR and is to be used as part of TNCL-SOP-OHS-0033, Emergency Call-Out Procedure to notify TNCL staff and contractors of an emergency that requires action from all staff. 2 types of emergencies are notified through the siren system; A continuous siren is activated when there is an immediate security threat or breach. On hearing the alarm every individual must take cover in their respective location, turn off phones and radios, and remain in situ until further instruction from the security team. An interrupted siren is activated when there is a fire or explosion incident that requires all individuals to evacuate to the site emergency assembly area for roll call.

5.14 Security Record Keeping

All security records and logs are stored within the Security Control Room for a period of 1 year. Following this, all records are archived in case of future requirements.

5.15 Journey Management

Comprehensive journey and travel management procedures are required to mitigate the risk for personnel accessing and egressing the site, and the early construction of the aerodrome to establish a fly-in-fly-out policy will avoid long and unnecessary road moves through risky terrain for the majority of staff.

6. THREAT CLASSIFICATION AND MANAGEMENT

6.1 TNCL Security Alert Levels

TNCL has adopted a system of categorizing the level of security alertness in each location at any time. Each security alert level is characterised by a set of security response actions.

Security Alert Levels describe the general level of assessed threat to a location (country, group of sites or single site). The base level Security Alert Level is "Low" (Green). An assessment of

Low means that a site is assessed to face no additional threats to those already considered during security planning, and the security measures implemented at a site are proportionate and sufficient.

At times the Security Alert Level might be increased, either project-wide or for a particular site or sites. The increased Security Alert Levels are "Medium" (Yellow), "High" (Amber) and "Extreme" (Red). These raised Security Alert Levels are designed to trigger the application of additional, generally temporary, security measures.

The four stages of security alertness are set out in an increasing order of preparedness:

Alert Level Green – Standard Operating Environment

A "Green" alert level should be in force at a site when the level of threat is assessed to be routine: that is when the threat is at a level that normally exists locally on a day-to-day basis.

Alert Level Yellow – Medium

Alert Level "Yellow" denotes an assessment by TNCL that the level of threat has increased to the extent that it is prudent to put in place additional security measures. An identified threat that may impact TNCL operations.

Alert Level Amber – High

Alert Level "Amber" denotes an assessment by TNCL that a threat against persons or property may be imminent, which will likely impact TNCL operations. An identified threat that will likely impact TNCL operations.

Alert Level Red – Extreme

Alert Level "Red" denotes an assessment by TNCL of a serious threat to the extent that hibernation, relocation, or evacuation of personnel is necessary along with the shutting down of operations. An identified threat that will imminently impact TNCL operations.

Pre-determined triggers are used to determine the appropriate Security Alert Level. These indicators can be seen in Table 5.

The appropriate security response measures suggested for each alert level are described in Table 6.

Table 5:TNCL Security Alert Levels

Alert Level	Definition	Triggers
Green (Low)	**Standard Operating Environment** A "Green" alert Level should be in force at a site when the level of threat is assessed to be routine: that is when the threat is at a level that normally exists locally on a day-to-day basis.	• All operations, business and lifestyle are running normally with employees going about their jobs with no or very limited restrictions. • The crime trend in the region and project is as expected. • There is no major travel or medical disruptions within the area.
Yellow (Medium)	**Caution** Alert Level "Yellow" denotes an assessment by TNCL that the level of threat has increased to the extent that it is prudent to put in place additional security measures. An identified threat that may impact TNCL operations.	• Increased civil disturbances within Kagera Region, but not directly targeting TNCL. • A non-violent labour protest or go-slow on or around TNCL project areas. • A noticeable change in atmospherics within project-affected communities. • Local community disturbances concerning social, health, safety, and environmental impacts. • A significant increase in local community or project security incidents. • Indicators of political instability in Tanzania, Burundi or Rwanda. • Sustained negative local/national/social media reporting of TNCL. • Public criticism of TNCL by International NGOs or Political Groups. • Civil disturbances along TNCL transit routes. • Any other event or situation that may impact the security of TNCL operations.
Amber (High)	**Warning** Alert Level "Amber" denotes an assessment by TNCL that a threat against persons or property may be imminent, which will likely impact TNCL operations. An identified threat that will likely impact TNCL operations.	• An actual threat has been identified against TNCL facilities or persons. • Civil disturbances targeting TNCL near company locations or transit routes. • Labour disturbances with threats or actual violence against TNCL staff or assets. • Site invasion on a large scale (more than 100 persons). • Reputational damage likely to lead to serious civil/labour disturbances targeting TNCL. • TNCL senior management/expatriate staff directly threatened. • An excessive use of force incident against community members by public/private security. • Potential impact of military conflict in the Region. • Any other event or situation that will likely impact the security of TNCL staff or operations.

Red (Extreme)	**Danger** Alert Level "Red" denotes an assessment by TNCL of a serious threat to the extent that hibernation, relocation, or evacuation of personnel is necessary along with the shutting down of operations. An identified threat that will imminently impact TNCL operations.	• Uncontrolled and violent Labour/Civil Disturbance on TNCL sites, with a loss of control of the situation by Private Security and TPF. • Breakdown of National law and order • National Coup or serious impact of regional military conflict. • Active and sustained violence targeting TNCL staff. • Diplomatic missions issue advisories that all staff and dependents should leave Tanzania. • Serious rioting and widespread confrontations between civilians and the authorities. • A perceived loss of control from GoT and TPF. • Any other event or situation with an imminent impact on TNCL staff or operations.

Table 6: Security Response Measures

Security Response	Low	Medium	High	Extreme
General Procedures	○ The TNCL Crisis Emergency Response Plan is in place and is maintained as a 'living document and updated periodically '. ○ The security situation is monitored. ○ Continue with routine work activities and standard security measures. ○ Ensure contingency and business continuity plans are current. ○ Annual Security Alert Level and Response Action training for GMs and Department Leads. ○ Establish relationships and liaison with local law enforcement. ○ Test panic alarms and emergency sirens monthly. ○ Design and establish a site haven and hibernation plan at each TNCL site. ○ Incorporate security awareness and information into business practices. ○ Advise all personnel to report the presence of unknown personnel and unidentified vehicles, abandoned packages and other suspicious activities.	○ Travel off the Project Area is restricted to necessary operational trips only, approved by the General Manager. ○ HAP escorts to accompany senior staff on Project Area Road moves. ○ Alternate travel routes and times. ○ Restrict movement into Tanzania to essential expatriate staff only. ○ Increase mobile patrols around the perimeter and vulnerable points. ○ ERT and TPF on stand-by notice to move. ○ Consider a request to station TPF officers on site. ○ Develop a Security Action Plan for the identified threat. ○ Review emergency and evacuation plans and test table-top rehearsal based on the security situation presented. ○ Develop contingencies for shutting down and evacuating office sites if necessary. ○ Prepare a safe haven for potential hibernation. ○ Stockpile additional supplies of water, non-perishable rations, fuel, and batteries ○ Concentrate High-Value Assets into centralized areas where security controls are tighter. ○ Check medical stores and facilities. ○ Avoid social activities off-site.	○ Travel off camp restricted to key business essential tasks only, approved by the GeneralManagerr and Security Manager. ○ All travel off-site to be accompanied by HAP/TPF escorts. ○ Freeze all expatriate movement into Tanzania. ○ Confirm the hibernation or evacuation plan if the alert level reaches 'red'. ○ Consider evacuation of non-essential staff. ○ Increase guard force numbers as required. ○ Deploy TPF to HVA facilities. ○ Consider halting mining operations. ○ Consider re-accommodating staff living in local villages to sites where security controls can be maintained. ○ ERT and TPF detachments are on full alert immediate notice to move status. ○ Medical staff on immediate notice to move status. ○ Double mobile patrols on all sites ○ Increase or redirect personnel to address critical emergency needs. ○ Implement business contingency and continuity plans as appropriate.	○ Full hibernation/ relocation based on the security situation. ○ Shut down all sites and operations.

			○ Staff to prepare a 'grab bag' in case of sudden hibernation or relocation requirement.	
Access Control	○ TNCL staff to enter sites using identity cards. ○ Vehicle offsite movement forms and material gate pass procedures in place ○ Ensure existing security measures are in place and functioning such as guarding, fencing, locks, CCTV surveillance, intruder alarms and lighting as appropriate.	○ Reduce access points to the minimum necessary for continued operations. ○ Close and lock doors, gates and barriers except those needed for immediate entry and egress. ○ Implement positive identification of all personnel; all bags are to be searched. ○ Inspect all packages being delivered. ○ Increase the frequency/percentage of vehicle checks on those entering office complexes, including vehicle cargo areas, and check the underside and other areas of vehicles where dangerous items could be concealed. ○ No motor vehicle to be left unattended adjacent to premises. ○ Weekly check of security systems to ensure they are functioning.	○ Full-time TPF presence at external access control points. ○ Augment security forces. Assign emergency response personnel: ○ Cooperate with authorities if they take control of security measures. ○ Neither private vehicles nor non-service vehicles are to be allowed to enter controlled premises or parking areas. ○ Postpone non-essential deliveries to premises. ○ No visitors are to be allowed access to the premises unless their visit has been previously authorized as being essential. ○ Routine maintenance and cleaning work to be suspended; such contractors to be prohibited entry. For extended periods of operation at this level, these tasks should be conducted under close supervision with additional validation from contractors.	○ No access/egress to sites other than for security, or approved movement by the Site General Manager and Security Manager. ○ Staff to remain in Safe-haven unless evacuation is authorised.
Communications	○ Maintain and test emergency communications monthly. ○ Maintain up-to-date contact details of appropriate agencies. ○ Wialon Satellite Tracking coverage on all vehicle movement. ○	○ Weekly CEMT report to be distributed. ○ Inform all external and internal stakeholders of the change in alert level. ○ CEMT meetings held weekly/as required. ○ Weekly test of emergency communication systems. ○ Review with staff the security measures, personnel safety and security details and	○ Daily CEMT report to be distributed. ○ Inform all external and internal stakeholders and key staff of the change in alert status. ○ Review with employees the plans, personnel safety and logistics requirements pertaining to the increased security level.	○ Emergency communications in full use to support hibernation or evacuation.

		logistics requirements pertaining to the increased security level. ○ Coordinate necessary security efforts with TPF authorities. ○ Consider consultation with local authorities about control of public roads adjacent to facilities.	○ Provide updates to staff on new security measures. ○ Maintain checks on communications equipment. ○ Coordinate necessary security efforts with TPF, advising them of the additional measures being employed.	○ Twice-daily CEMT update to be provided.

6.2 Communication of Security Alert Levels

The Security Project Manager will ensure that project staff, contractors, and visitors are informed of the current Security Alert Level. Avenues used for this communication will include:

- Security Alert plaque located outside the site security office and main gate indicating the current Security Alert Level.
- Updates at site daily management meetings.
- Reporting in daily, weekly and monthly security reports.
- Site Safety Induction

6.3 Responsibility for altering the Security Alert Level

Alteration of the security alert level at the site is the responsibility of the Site General Manager. Should a generalized, country-wide escalation of the security alert level be required, the TNCL Country Manager will make the final decision.

Procedure for altering the Security Alert Level

If a threat is identified whereby consideration is required for elevating the Security Alert Level beyond "Low" (Green), the Security Project Manager will:

- Immediately notify General Manager.
- Provide a detailed briefing to the General Manager of the security situation and possible impacts.
- Advise General Manager on the correct security alert level for the situation.

General Manager, after assessing the information provided, and consulting with other members of the Crisis Emergency Response Team will make the decision to remain at the current alert level or escalate to the level required:

- General Manager will inform the TNCL Country Manager of the new Security Alert Level and intended Response Actions.
- The Security Project Manager and Site General Manager communicate to the Crisis and Emergency Response Team describing the situation and required response actions based on the new alert level.
- All CERT members will be prepared to implement the TNCL Crisis Emergency Management Plan.

7. INCIDENT AND EMERGENCY MANAGEMENT

The priority in resolving any emergency incident and for business continuity management will always be:

- The safety and security of people.
- The protection of assets.
- Adherence to the law.
- The timely reactivation of business functions.

The TNCL Crisis and Emergency Response Plan (CERP) with the Crisis and Emergency Response Team take overall responsibility for all emergency incidents affecting all or significant elements of TNCL's operations.

The management of security incidents are guided by two TNCL Standard Operating Procedures:

- TNCL-OHS-SOP-0033, Emergency Callout Procedure.
- TNCL-OHS-SOP-0002, Incident, Injury Reporting and Investigating.

Tembo Nickel has categorized emergencies into three main groups, namely Security, Medical and other emergencies that require Emergency Response Team involvement.

7.1 Means of Notifying

7.1.1 Panic Button Alarm

All rooms and offices at Tembo Nickel site have a mounted panic button which are tested on a monthly basis. A panic button will be activated when a staff member identifies a security, medical or other emergency which communicates a direct alarm to the security control room.

On hearing the alarm, the Security Control Room operator will inform the site security manager of the alarm and the exact location of the alarm. The site security manager and control room officer will coordinate the security team to visit the alarm location to understand the nature of the emergency and what assistance is required.

7.1.2 Emergency Call Flow Chart

Tembo Nickel has adopted an emergency call flow chart to ensure that the correct procedure is followed, and correct persons are notified in the event of a security incident.

Figure 13: Emergency Call Flow Chart

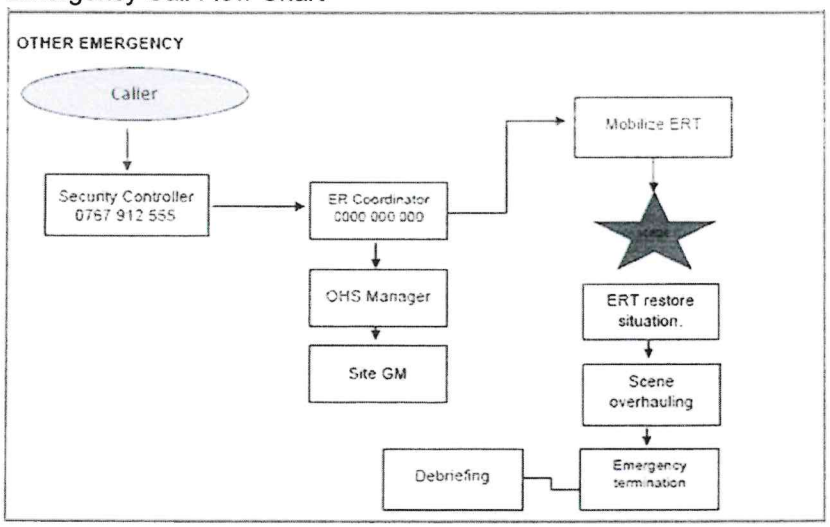
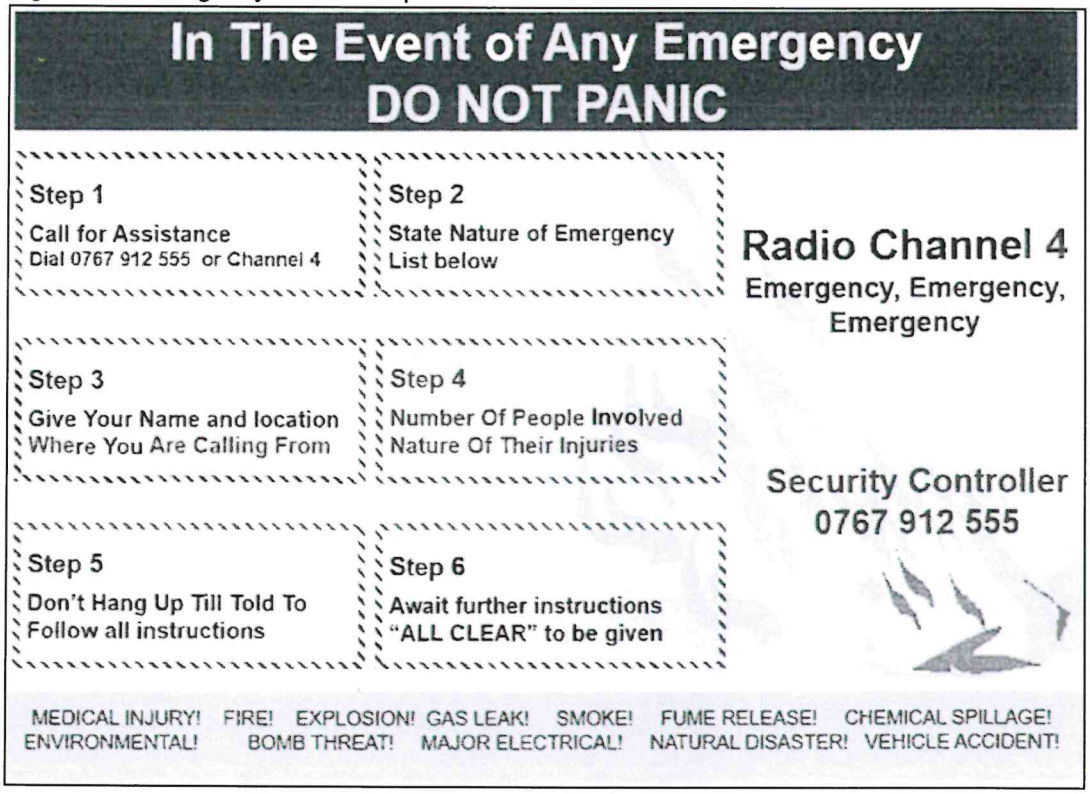


Figure 14: Emergency Callout Steps



7.2 Means of Alerting

Tembo Nickel has adopted a siren system in the event that all staff are required to be notified of a security emergency:

Continuous Siren: A continuous siren is activated when there is a security threat. The siren button is situated inside the control room and is to be activated by the Security Control Room Officer on the instruction of the Security Project Manager, Site Security Manager, General Manager, OHS Manager, or Emergency Response Team leader.

Interrupted Siren: An interrupted siren is activated when there is a fire or explosion incident that needs staff to evacuate to the Assembly Point for roll call.

7.3 Security Incident Reporting

All Security incidents will be reported to the TNCL General Manager within 24 hours of occurrence using the designated Incident Report Template (Annex A). High potential incidents require an immediate Flash Report to be sent out to department leads and GMs. An assessment by the Security project Manager, OHS Manager, and Site General Manager will determine the severity of the incident and the requirement of a Flash Notification.

7.4 Security Investigation Reporting

A security Investigation report will be submitted by the contracted security provider within 7 days of a security incident including findings, recommendations, and action plan. The security investigation report will be reviewed and signed off by the relevant TNCL department manager, and all individuals with action points will be informed.

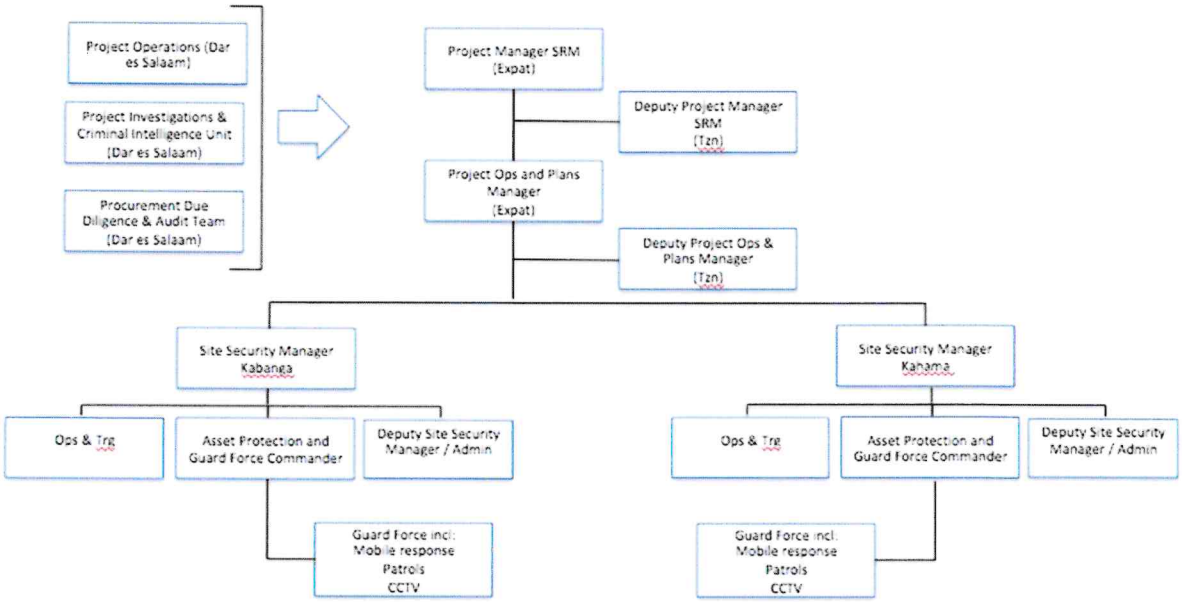
7.5 Security Incident Records

Copies of Security incident reports, investigation reports, and proof of actions completed will be filed within the TNCL Security Incident folder with the overarching TNCL Security Incident Index .The file will be maintained and audited by the Security Project Manager on a quarterly basis to ensure compliance.

8. SECURITY MANAGEMENT AND CONTROL

8.1 Management Structure

Figure 15: HAP Management Structure



8.2 Deliverables

Project Manager

- Oversight responsibility of the security strategy
- Develop, implement and maintain the Security Management Plan
- Develop security plans and strategy for new facilities
- Design Security Best Practices
- Maintain, review and update the project Security Risk Assessment
- Country level emergency/crisis preparedness advisory and oversight
- Advise the Country Manager and crisis management team on risk escalations and appropriate responses
- Monitor, communicate and advise on the appropriate security risk level at TNCL locations
- Internal and external security stakeholder identification and liaison

Project Operations Manager

- Management of security operations
- VPSHR compliance, training and monitoring
- Site emergency response oversight
- Develop the security training program
- Travel procedures
- Overseeing the implementation of the Security Management Plan
- Maintaining security standards stipulated within the Security Management Plan
- QA/QC reporting
- Manage critical infrastructure security upgrade projects
- Ensure safety procedures are adhered to
- Site Security Plans, SOPs and post Instructions
- Crisis Management training and rehearsals
- Visitor and arrival procedure and briefing
- Regional Tanzanian Police Force liaison and relationship

Site Security Manager Kabanga/Kahama

- Day-to-day operational security management on-site
- Ensure the effective execution of the procedures stipulated within the SMP
- Respond to security incidents and coordinate appropriate notification and proportionate immediate response
- Ensure the timely reporting of security incidents
- Monitor guard force for VPSHR compliance
- Daily supervision of the Asset Protection Team
- Control the reporting of security faults
- Liaise with equipment maintenance contractors to ensure regular servicing
- Conduct security staff and equipment auditing
- Ensure access control measures and asset protection procedures are enforced
- Report all personnel related matters and disciplinary infringements to the project manager.

Ops and Training

- Operational support to the SSM
- Project Security Planning

- Support the design and maintenance of security SOPs
- Develop, and maintain project security training program
- Deliver core security refresher training as per the training program within the Security Management Plan
- Support the delivery of security and project VPSHR training
- Lead the new-joiner security training program

Administration Lead/Deputy Site Manager

- Assume responsibilities of SSM in their absence
- Manage security roster
- Receive security grievances for investigation
- Lead recruitment process for new joiners
- Manage ID card issuance
- Maintenance of staff P-files

Asset Protection and Guard Force Commander

- Enforce all security SOPs on TNCL facilities
- Identify and report all vulnerabilities on TNCL facilities to the site security manager as they become known
- Deploy and ensure guard force numbers are correct for each shift.
- Daily post checks for uniform and equipment compliance.
- Provide two daily briefings to the guard force on muster parade
- Ensure TNCL security and safety policies are adhered to by security personnel
- Monitor VPSHR compliance
- Report safety hazards identified on site to the OHS department
- Be prepared to assist OHS in fighting fires on site

Project Operations Room, DSM

- Regional monitoring of TNCL vehicle tracking, CCTV, access control, and other remote monitoring systems
- Organizational journey management oversight
- Security incident management and response coordination
- Liaison with Emergency Services of TZ

- Emergency Point of Contact for TNCL, contractors and VIP visitor travelling in to, out of, or within Tanzania.
- Daily media/information reporting
- Flash notifications of local, regional, national incidents provided for management and travellers

Project Investigations and Criminal Investigation Unit

- External team to investigate security incidents
- Full investigation to be completed on request from TNCL
- Investigation reports to be submitted to TNCL HR GM
- Support and provide evidence during investigation hearings
- Ensuring investigation are completed within the laws of TZ
- VPSHR compliance monitoring of suspects in private or public security custody

Procurement Due Diligence and Audit Team

- Review Procurement activity and processes
- Provide audit reporting based on findings
- Identify opportunities to update and improve service agreements and processes, improving procurement performance
- Identifying fraud or system errors
- Identify risks within the TNCL supply chain
- Targeted auditing based on information and suspicions

9. PRIVATE SECURITY MANAGEMENT

9.1 Private Security Role

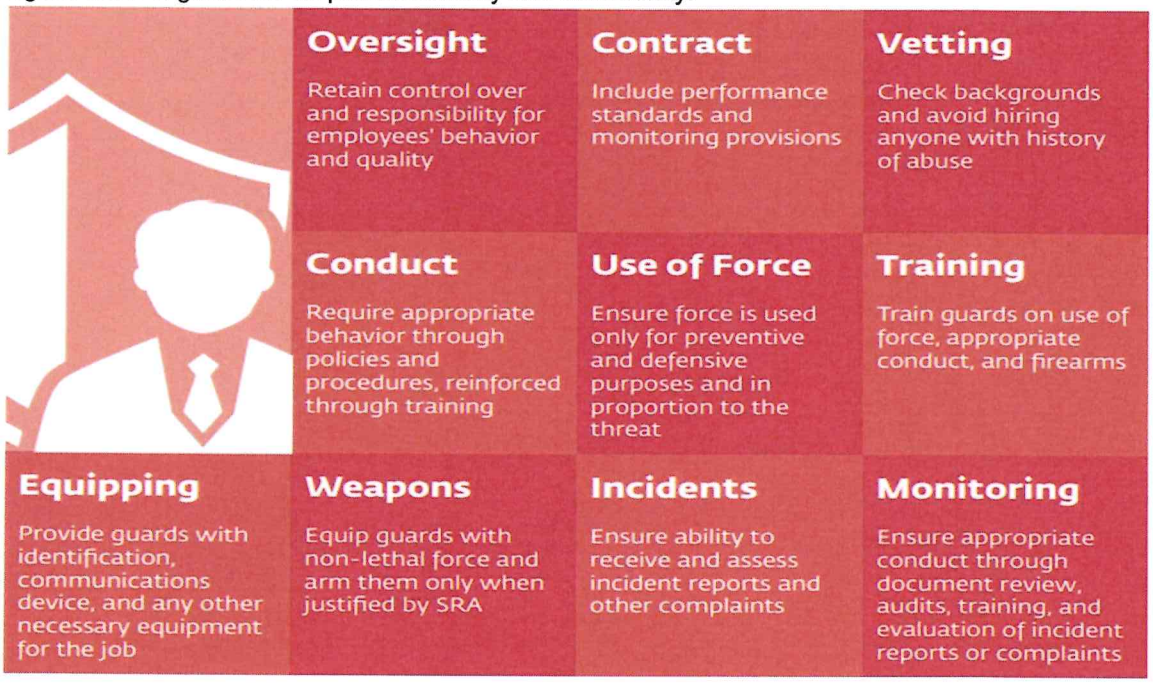
The separation of roles and responsibilities between private and public security must be understood and put into practice, whereby private security provides internal security and public security secures the area beyond the perimeter and manages the community security. Clear lines of accountability are defined for each security function within the TNCL TPF MoU.

The private security function is unarmed and exercised within a defined perimeter boundary. The role of the private security team is that of asset protection, access control, incident

response, and crisis management support to TNCL. The private security personnel do not have law-enforcement authority and will not encroach on the duties, responsibilities, and prerogatives reserved for public security forces.

Tembo Nickel is guided by good international practices in relation to hiring, rules of conduct, training, equipping, and monitoring of such contractors:

Figure 16: IFC guidance on private security and community.



9.2 Provision and Composition of Private Security

From 1st February 2023, Henderson Asset Protection were awarded the contracted private security provider for TNCL. A full tender, vetting and selection process was conducted for the security contract award, with findings and report sent to the Tanzanian Mining Commission as per national legislation. Local content is a high priority where preference to qualified Tanzanian candidates is given where possible, and further preference for those applicants from the Kagera Region and Ngara District. Diverse hiring practices are promoted, including gender and indigenous inclusiveness.

Henderson Asset Protection, as of 15 May 2023, are delivering an optimised guard force of 72 staff to secure the internal perimeter of the existing mine camp, drill camp and sensitive areas. The guard force is organised according to their assigned posts with a Site Security

Manager (SSM) in charge of the security commanders who in turn will monitor the activities of the guards assigned to the posts. The commanders are accountable to the SSM for attendance and performance of all guards under their control. The guards are accountable to the commanders for adherence to general orders and post orders specific to their respective post. The guard force accomplishes inter-post coordination through orders, memoranda, and radio communications. All guards are required to provide mutual support and emergency response in accordance with Standard Operating Procedures.

The below deployment chart shows the breakdown of posts/positions:

Table 7: Deployment Chart

Position	Day	Night	Off	Total
Site Security Manager	1	0	0	1
Deputy Site Security Manager	1	0	0	1
Guard Force Commander	1	0	0	1
Ops and Trg Commander	1	0	0	1
Shift Commander	1	1	1	3
MRU Commander	2	2	2	6
MRU Driver	2	2	2	6
MRU Officer	4	4	4	12
Security Control Room Operator	1	1	1	3
Security Officer	10	16	11	37
Admin Support Clerk	1	0	0	1
Total	**24**	**26**	**22**	**72**

9.3 Background Screening

Recruits for security positions will have a security background from Tanzanian military, police, vetted community security positions, or private security experience. Priority and consideration will be given to local hire from project-affected areas. All personnel are meticulously screened, and all staff will need to have met certain standards including:

- Pre-Employment screening
- Past Employment review: Prior jobs held, level of performance, reasons for

employment termination and concept of his direct superior. This includes verification of military records.

- Judicial review: Criminal records, fines and lawsuits.
- Security screening for association with terrorist/threat groups.
- ID checks
- Local guarantor and community leadership letter of approval
- Driving record review: For candidates who apply for Guard/Driver posts, their driving record will be verified.
- Education review: Verification and level of accomplishment.
- Police background check.
- Financial checks: Verification of existing bank accounts, level of debt (if any) and debt payment capacity analysis.

Candidates must pass the recognized Basic Security Guard Course, training screening evaluations, along with a routine physical examination before an offer of employment is made. Additional role-specific training is detailed in the Training Plan. Any potential employee found to have been implicated in past human rights abuses during the hiring and on-boarding process will not be offered employment with HAP.

9.4 Voluntary Principles on Security and Human Rights

The contracted private security provider HAP, provides an unarmed security service which respects the rights and dignity of all people, complying with all legal requirements. All security operations are carried out in compliance with VPSHR, the Universal Declaration of Human Rights, the relevant national and international regulations and will:

- respect internationally recognized human rights as set out in the international Bill of human rights and the International Labour Organisation's Declaration on Fundamental Principles and Rights at Work.
- recognise our responsibility to respect human rights and avoid any complicity in human rights abuses, as level in the UN Guiding Principles on Business and Human Rights.
- treat people fairly and without discrimination and respect the rights of people in communities impacted by our activities.
- seek to identify the impact of adverse human rights and take appropriate steps to avoid, minimize or mitigate them.
- Applicable Human Rights Principles are covered throughout the training program with

special attention on the VPSHR, Use of Force, Arrest and Detention, and Code of Conduct.

TNCL and their private security provider additionally commit to operate in accordance with the International Code of Conduct for Private Security Providers (ICOC). TNCL commits:

- to operate in accordance with the Code.
- to operate in accordance with applicable laws and regulations, and in accordance with relevant corporate standards of business conduct.
- to operate in a manner that recognizes and supports the rule of law; respects human rights and protects the interests of their clients.
- to take steps to establish and maintain an effective internal governance framework to deter, monitor, report, and effectively address adverse impacts on human rights.
- to provide a means for responding to and resolving allegations of activity that violates any applicable national or international law or this Code; and
- to cooperate in good faith with national and international authorities exercising proper jurisdiction, regarding national and international investigations of violations of national and international criminal law, of violations of international humanitarian law, or of human rights abuses.

VPSHR training, approved by TNCL, will be provided to every private security staff member prior to deployment on TNCL sites. Official VPSHR training records will be maintained and stored by the HAP project manager.

9.5 Use of Force

The use of force by private security is only sanctioned when it is for preventive and defensive purposes in proportion to the nature and extent of the threat. Use of Force training is provided to each security contractor prior to deployment at TNCL sites, based on the principles of force being necessary, proportional, and reasonable. Annual refresher training will also be provided with records maintained by the security project manager. HAP private security are not armed with lethal weapons.

- In the event a security guard is required to use force against the individual, the security guard shall:
- Attempt non-violent means first and only use force when necessary.
- Use only the minimum of force required, to affect the purpose and keep it proportional to the threat.
- Operate strictly within the law and the authority is given to them to use force.

- Clearly prioritize the prevention of injuries or fatalities and peaceful resolution of disputes.
- Render medical aid to an injured person, including offenders.
- Report any use of force as soon as possible to Security Manager; and
- The use of force may need to be justified in any later hearing. The Security Manager will have the responsibility of presenting the justification following any reportable incidents.

9.6 Training

TNCL and HAP commit to maintaining the highest standards of guard force technical and professional proficiency through comprehensive pre-deployment, and continuation compliance training plans. The Voluntary Principles on Security and Human Rights guide and underpin all security training. Training records will be kept and provided to TNCL upon request and open to inspection and audit.

Training of the private security team will be designed and delivered by the Project Ops and Planning Manager, with the support of the Project Manager and both deputies. The project will ensure that security personnel receive procedural or knowledge training in:

- Basic guarding skills
- Guard-post orders and procedures
- Proper conduct and ethics/human rights
- VPSHR
- Rules for the use of force
- Non-lethal equipment training
- Health, Safety, and Environment (HSE) mandatory training
- Conflict Resolution
- Public order training
- Site specific security operating procedures
- Site incident response
- Fire incidents
- Client Etiquette
- Communications
- Role specific security responsibilities

Security commanders and above shall receive additional security management training covering the following modules:

- Module 1: Security and Risk Overview
- Module 2: Managing the Security Function
- Module 3: Leadership and Managing Personnel
- Module 4: Crime Prevention
- Module 5: Security Risk Assessment
- Module 6: Security Design and Audit
- Module 7: Advanced VPSHR
- Module 8: Security Reporting

Further training needs will be identified when:

- Standards fall below those acceptable to HAP/ TNCL
- Reorganisation, new techniques and/or technology make it necessary to train those concerned in new skills.
- Promotions, transfers, career development (i.e. actual or anticipated changes in the role of an employee or group of employees) occur.
- Changes in project specifications that mean the development of new skills are required.
- Changes in project requirements.

9.7 Equipment

Private security guards will be provided with the following equipment for their duties:

Uniform: The uniform items will be furnished in the required quantities and replaced routinely to ensure a professional appearance. Standard items include:

- Shirts
- Trousers
- Belt
- Beret
- Sweater
- Lanyard
- Boots
- T-shirt
- Cap

Personal Protective Equipment: Serviceable PPE will be provided to each security officer to safely complete their duties. The minimum PPE to be provided will be:

- Hard Hat
- Eye Protection
- Safety Boots
- Hi-Vis vest
- Raincoat
- Rain Boots

Daily Equipment: The following equipment will be provided to security officers for their daily shift:

- Whistle
- Torch
- Notebook
- ID Card
- Baton
- Baton Holder
- Handcuffs

9.8 Grievance Reporting Mechanism

Good practice regarding the use of security forces is based on the concept that providing security and respecting human rights can and should be consistent, with grievance redress procedures central to this approach in ensuring negative interactions or concerns between private security and TNCL staff, contractors, and the local community are understood and managed. The implementation of an effective grievance reporting mechanism at a timely investigation of any alleged unlawful acts from project staff, contractors, and security personnel support a VPSHR compliant and transparent private security operation.

TNCL have implemented a proactive and comprehensive Grievance Reporting Mechanism Procedure and provided community outreach programs to educate the project affected people on acceptable behaviour by TNCL security personnel, and how and where to go with complaints about the conduct of security personnel. Further information can be found in Section J.

Internally, HAP has formal grievance procedures in place to handle payroll, harassment and other grievances that occur while managing a guard force. Grievance and escalation

procedures are appropriate to the type and nature of the grievance and conform with Tanzanian labour laws and legislations. Senior management take a keen interest in ensuring that grievances are resolved and any necessary remedial actions including disciplinary actions and terminations are carried out.

10. MANAGING RELATIONS WITH PUBLIC SECURITY

10.1 Public Security Role

The Police are vested under the law with the sole responsibility in Tanzania of ensuring public security and safety; protecting life and property; preserving order and preventing the commission of offenses; bringing offenders to justice through investigation, apprehension, detention and processing of persons suspected of criminal offences; and involving the community in the policing process to create an environment that builds an effective working relationship between the community and the Police and which has respect for human rights and fundamental freedoms.

The provision of assistance of the TPF will focus on providing a service to improve law and order in the local communities before, during and after the expected influx of project-induced migrants to Ngara District. TNCL, being a part of the community may also request support from public security, the same as any other resident. The Police shall be stationed at Bugarama Police station outside of the TNCL project and SML area and shall only enter its private facilities on request of the TNCL, when a significant security threat arises that the private security within the site are not capable of legally or practically responding to, or pursuant to a lawful criminal investigation.

As a matter of principle TNCL will not be involved whatsoever in any policing, military activities, paramilitary activities, or armed conflicts that may occur anywhere in the vicinity of the SML. Police personnel will be adequately and properly supervised by their own chain of command, and without the involvement of TNCL or its personnel.

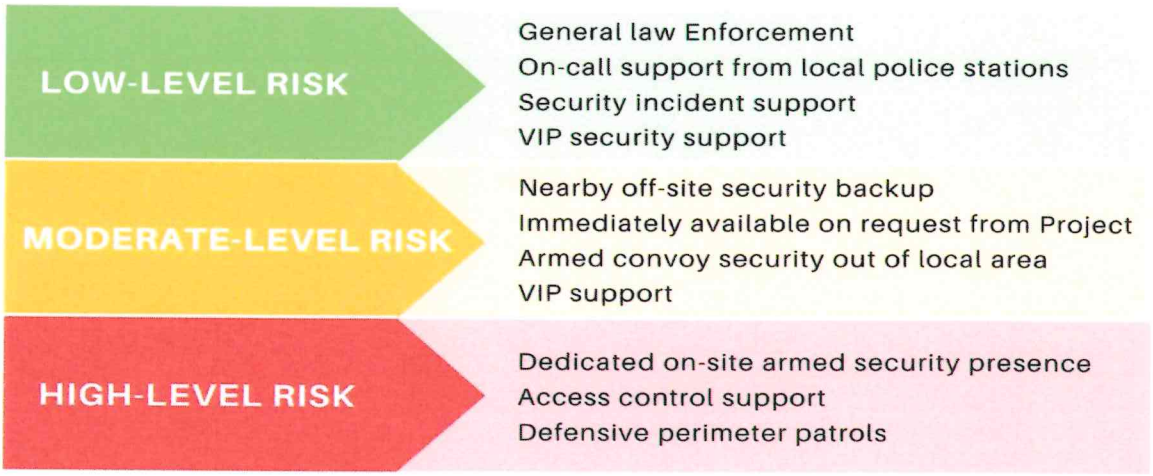
10.2 Memorandum of Understanding

A memorandum of understanding is a formal, written agreement between the company and the government and/or its public security forces, which establishes, and documents agreed key expectations and decision-making processes and procedures. It allows the company, government, and public security forces to delineate their respective roles, duties, and

obligations regarding security provision.

An MoU between TNCL and the Tanzanian Police Force was signed on 12 May 2023, outlining the above role of the local police and the initial support to be provided by TNCL. The MoU emphasizes the VPSHR, as well as national and international law, and includes references to international standards and company policies. TNCL are guided by IFC performance standard 4 recommendations on managing the relationship between the company and public security forces, with a flexible MoU ensuring that the level of support to be received from the Tanzanian Police Force is assessed using a risk-based approach.

Figure 17: IFC Guidance on Risk Based Use of Public Security



10.3 Provision and Composition of Public Security

As per the MoU agreement the TPF will provide an additional section of officers to support the security for the local communities. TNCL acknowledge that crime and other risks to these communities will increase as a result of project-induced in-migration. Therefore, as part of the MoU agreement TNCL have agreed to rehabilitate Bugarama Police Station to the standard of a 'Class B' facility in order to facilitate the additional police in the area. A class B facility is defined under Tanzania Police General Orders as

An outpost has been agreed to be constructed along the TNCL Southern Access Road, to support community security to the south and east side of the project.

The additional section of officers comprises of:

- One Officer in Command
- One Second in Command
- Four male officers

- One driver
- Two Female officers

One vehicle will also be provided to the TPF by TNCL. The vehicle offered to TPF shall be solely an asset of TPF and be used for official purposes only, as documented in the MoU.

10.4 Use of Force

As stipulated in the MoU agreement between the TPF and TNCL, Police officers or other Police personnel deployed to the TNCL project area will have been provided with training on the applicable Human Rights Principles and international humanitarian law and international security and human rights standards related to the use of force (e.g. UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials) in accordance with the guidance set out in the VPSHR.

Police deployed to the area will only use weapons as a last resort to protect the lives of police officers or others and, if such weapons are to be used or such acts are to be committed, then they are to be used or committed only in a manner that takes into account and limits the risks of danger to other people who are not involved.

Where Police officers are requested to enter the corporation's mining areas, they have agreed through the MoU observe all company security and safety policies. Weapons will not be visible or carried unless essential for the protection of the corporation's staff.

10.5 VPSHR

The Police are required to abide by the Tanzanian law and Tanzania's international legal obligations, including in relation to respect for human rights and fundamental freedoms, and to cooperate with the Tanzanian Commission for Human Rights and Good Governance ("CHRAGG").

The voluntary principles on security and human rights are at the centre of the MoU agreement between the TPF and TNCL, and the VPSHR will be at the forefront of the TNCL security operation. Any reported grievance of public security VPSHR violations through the GRMP will be reported to the Regional Police Commander Kagera for investigation.

As per the MoU agreement, police stationed and working within the project area agree to complete additional VPSHR workshops and information sharing sessions led by TNCL within 7 days of arrival into the area. Training forms are completed and filed by HAP to maintain records.

Figure 18: TPF attending a HAP led VPSHR information sharing exercise.

10.6 Training

Police officers or other police personnel will have received suitable and adequate training in accordance with the police training methods and requirements before being deployed in the area.

All training on the Applicable Human Rights Principles, international humanitarian law, International Security and Human Rights Standards related to the use of force will include how to implement the Security and Human Rights Standards, including the following Core Competencies:

(i) an awareness of the Security and Human Rights Standards as they apply to Government Security Force personnel, including international human rights and humanitarian law and international law enforcement principles.

(ii) an understanding of, in the event of any violation or abuse of human rights, the legal consequences for the particular individuals involved, the Government Security Force, and Corporation.

(iii) knowledge of common scenarios in which violations and abuses of the law and international protocols and conventions might take place; and

(iv) awareness of and an ability to apply the procedures that Government Security Force personnel should follow in order to avoid such violations and abuses, including practical steps to take in the context of security incidents, protests, or strikes on, in the vicinity of, or related to the project area.

Government Security Force agrees to share information with TNCL upon request that demonstrates that Government Security Force personnel received the training and met the Core Competencies.

As well as the VPSHR training level above, TNCL may also request that police drivers are provided with safety and advanced driver training delivered by the company.

10.7 Incident Reporting

The TPF have agreed to promptly advise the TNCL security representative of any security incident involving the use of weapons or use of force within the project affected areas. Police will report to a senior police officer any incident that has caused any injury, death, or substantial damage to property, who will immediately notify the TNCL designated liaison person. A daily briefing on police activities and relevant observations in the area will be provided to the TNCL liaison person by the police commander or designate.

10.8 Grievance Reporting Mechanism

Good practice regarding the use of security forces is based on the concept that providing security and respecting human rights can and should be consistent, with grievance redress procedures central to this approach in ensuring negative interactions or concerns between public security and the local community are understood and managed.

TNCL have implemented a proactive and comprehensive Grievance Reporting Mechanism Procedure and provided community outreach programs to educate the project affected people on acceptable behaviour by public personnel, and how and where to go with complaints about the conduct of police personnel.

As per clause 10 (e) in the MoU agreement, TNCL may report any credible allegations of human rights violations to the appropriate authorities and agencies, and it shall investigate any complaints received against police officer or other police personnel. TNCL retain the right to request that an individual officer is removed from the area should there be evidence or strong suspicion of a VPSHR violation.

11. COMMUNITY BASED POLICING

11.1 CBP Role

Community policing (Polisi jamii) was officially introduced in Tanzania in 2006 as part of an ongoing police reform Programme. In addition to attempting to improve communication between police and the public, the police have promoted participatory security, whereby citizens are encouraged to form 'neighbourhood policing' institutions to prevent and detect crime.

TNCL mining operation will only be successful if a social license to operate exists. CBP strategies can empower local leadership and policing structures, provide additional community safety and security, and build relationships between the project and the affected villages. A TPF-led CBP Programme will assist the police at the grass roots level and provide early warning and information for the TNCL Security Risk Management team of actual and potential risks to the project.

Community Based Policing structures already exist in Kagera region, and in some form in most communities in the TNCL project affected communities. TNCL intend to support the TPF to lead and improve on the existing structures to increase the capacity of the community to deal with local crimes help to offset the risks associated with in-migration. Further goals of the CBP program are to improve police-community relations in the project affected communities and support the TPF to improve preventing and solving crime.

Should there become an increase in cross-border banditry again in the future, CBP structures can provide valuable early warning and reporting to the TPF, who then can provide a quicker response with improved and reliable information from the CBP team.

11.2 CBP Structure

The Community Based Policing strategy and structure is currently in development and will be updated on completion.

11.3 CBP Relations

The idea and organisational strategy of CBP is both a way of thinking and a strategy that allows a group of stakeholders, the police, the private sector, local government authorities and the community to work closely together in creative ways to solve the problems of crime and other actual or perceived threats to the community.

Currently the TNCL risk management team are forging relationships with village leadership and current community policing structures to build and maintain relations between TNCL and local community security teams.

12. GRIEVANCE REPORTING AND INQUIRY

12.1 Tembo Nickel GRMP

The UN Guiding Principles on Business and Human Rights, IFC and the ICMM requires that an external stakeholder grievance and conflict resolution mechanism is implemented, and requires a clear mechanism for registering, evaluating, and resolving all issues and complaints.

Tembo Nickel Corporation is committed to transparency, account and participative processes with local communities of the project area of Ngara District, particularly those communities impacted by the project, called the 'social influence area'. The social influence area includes communities in the wards of Bugarama, Rulenge, Bukiriro and Muganza, as well as Nyakahura Ward in Biharamulo District. The social influence area may also include communities along the road to the town of Ngara as there will be increased traffic. Also, often times there is some project or employee activity in these areas. This also applies to the southern access road.

To help fulfil this commitment, a grievance policy has been established, a complaints management system and complaints log to track closure of community complaints and satisfaction of the stakeholders involved. The grievance policy and community complaints management system, developed and tested during prefeasibility phase (PFS), are intended for use in construction phase. The Tembo Nickel grievance policy and procedures builds on the former system to ensure consistency and tracking ability.

The TNCL grievance policy is governed by the Sustainable Development Standards and Sustainable Development Policy of Tembo Nickel. It is adapted to the cultural context of Ngara District and the scale of the Tembo Nickel Project with regard to risks and level and type of impacts.

12.2 Complaints Procedure

The purpose of the complaint's procedure is to ensure that all complaints from local stakeholders are dealt with appropriately, with corrective actions being implemented and the complainant being informed of the outcome in a timely manner. All complaints will be handled in accordance with the flow chart below:

Step 1: Complaint Received

- Verbally or in writing
- Record report and date on Grievance Log

Step 2: Complete Grievance Record Form

- Part A and B: Document SOP2_TN_CR_GRM_Record_Template

Step 3: Complete Immediate Action Section

- See document OP2_TN_CR_GRM
- Assign Responsibility

Step 4: If Immediate Action resolves grievance

- Inform grievant of proposed corrective action
- Record date on grievance log
- Close out of grievance record form (Part E)
- Record, sign and close grievance with a grievance resolution closure agreement (SOP3_TN_CR_GRM_Closure_Agreement_Template)
- Record closure date on grievance log

Step 5: If immediate Action does not resolve grievance

- Establish long term corrective action- Part C in document SOP2_TN_CR_GRM_Record_ Template
- Establish follow up details- Part D in document SOP2_TN_CR_GRM_Record_ Template
- Record Date on grievance log
- Inform grievant of long-term corrective action
- Implement corrective action
- Carry out follow up of corrective action
- Confirm corrective action satisfies grievant (if no restart process)
- Record date on grievance log
- Close out of grievance record form (Part E)

- Record, sign and close grievance with a grievance resolution closure agreement (SOP3_TN_CR_GRM_Closure_Agreement_Template)
- Record closure date on grievance log

12.3 Inquiry and Documenting Procedure

Table 8: Inquiry and Documenting Procedure

<table>
<tr><th colspan="4">Procedure step-by-step</th></tr>
<tr><td>Step 1</td><td colspan="3">Complaint received
Verbally or in writing</td></tr>
<tr><td></td><td colspan="3">a) Record Date on Grievance Log</td></tr>
<tr><td>Step 2</td><td colspan="3">Complete Grievance Record Form (Part A and B)
See document: SOP2_TN_CR_GRM_Record template</td></tr>
<tr><td>Step 3</td><td colspan="3">Complete Immediate Action Section and assign responsibility (Part C)
See document: SOP2_TN_CR_GRM_Record template</td></tr>
<tr><td></td><td colspan="3">Immediate action enough to resolve grievance</td></tr>
<tr><td></td><td>If Yes</td><td colspan="2">If No</td></tr>
<tr><td></td><td rowspan="8">a) Inform grievant of proposed corrective action</td><td colspan="2">a) Establish long term corrective action,
(Part C in SOP2_TN_CR_GRM_Record template)</td></tr>
<tr><td></td><td colspan="2">b) Establish follow-up details
(Part D in SOP2_TN_CR_GRM_Record template)</td></tr>
<tr><td></td><td colspan="2">c) Record Date on Grievance Log</td></tr>
<tr><td></td><td colspan="2">d) Inform grievant of the proposed corrective action.</td></tr>
<tr><td></td><td colspan="2">e) Implement corrective action</td></tr>
<tr><td></td><td colspan="2">f) Carry out follow-up of the corrective action</td></tr>
<tr><td></td><td colspan="2">g) Corrective action satisfies grievant</td></tr>
<tr><td></td><td>If Yes</td><td>If No</td></tr>
<tr><td></td><td>Inform grievant of proposed corrective action</td><td rowspan="5">Restart process from above path for Step 3 Immediate action not enough a) and renegotiate</td></tr>
<tr><td></td><td colspan="2">b) Record Date on Grievance Log</td></tr>
<tr><td>Step 4</td><td colspan="2">Close out of Grievance Record form (Part E)</td></tr>
<tr><td></td><td colspan="2">a) Record, sign and close grievance with a Grievance Resolution Closure Agreement
See document: SOP3_TN_CR_GRM_ClosureAgreement template</td></tr>
<tr><td></td><td colspan="2">b) Record Date on Grievance Log</td></tr>
</table>

13. COMMUNICATIONS PLAN

All TNCL facilities and vehicles should be fitted with appropriate communications systems which enable instant passage of communications to and between security personnel and across departments. Communications systems should enable security personnel and drivers of vehicles to pass on critical time-sensitive information, incident reporting and communicating a response to deploy a quick mobile response unit. All radios must be regularly mustered and tested to confirm that they are operational. The following systems should be employed:

13.1 SML Area Tactical Communications Network

Very High Frequency (VHF) Radio communications are required for local site security. This comprises of handheld DP4801 Motorola radios issued to key posts and security staff, and Motorola Base Station DM4401e digital radios in the security control room and mounted to TNCL vehicles.

13.2 Country-wide Communications Network

High Frequency (HF) Radios does not yet exist in the TNCL communications plan but will be introduced during the construction phase ready to cover the transport network between Ngara and Kahama in the operational phase.

13.3 Key Staff Members and Lone Workers

Satellite communications: In the event of a cellular network failure or sabotage, satellite phones provide an emergency communication backup not reliant on national infrastructure. Thuraya XT Pro Satellite phones should be issued to TNCL security patrols, key managers, and transport vehicles that operate in communication black spot areas.

13.4 Satellite Tracking

An effective vehicle tracking system provides a journey management capability to an organisation to monitor the fleet's movement and provides alerts when vehicles are over-speeding, away from expected geofences, and where panic buttons are installed providing a method of communicating an emergency to the security control room. Fuel tracking systems provide a valuable tool in preventing fuel theft, and safety features such as pre-start alcohol testing and seat belt monitoring are available to improve journey OHS.

13.5 Mobile Phones

Mobile Phones will be issued to key appointments, as a secondary means of communication. Mobile phones are unreliable and may fail at a critical time or in the event of an outbreak of conflict. Over-reliance should not be placed on this form of communication.

Table 9: TNCL current Communications Plan

TNCL COMMUNICATIONS PLAN- CURRENT STATUS

MOTOROLA HAND HELD VHF RADIOS

Radio No	Owner	Call Sign	Area of Assignment	Serial Number
1	GM	Golf Mike	General Manager	871TRPC729
2	Security	Papa Mike	Project Manager	871TRPD174
3	Security	Sierra 1	Site Security Manager	871TRPE310
4	Security	Sierra 2	Deputy Site Security Manager	No Radio
5	Security	Sierra 3	Ops and Trg Cmd	No Radio
6	Security	Sierra 4	Guard Force Commander	871TRPD540
7	Security	Zero	Security Control Room	821TUV4752
8	Security	Charlie 1	Duty Shift Commander	871TRPE279
9	Security	Charlie 2	Main Gate	807TVH4367
10	Security	Charlie 3	Core Yard	871TRMD163
11	Security	Delta 1	Drill Camp	807TVRP772
12	Security	Delta 2	Rig Site 1	807TVRP788
13	Security	Delta 3	Rig Site 2	807TUH0152
14	Security	Delta 4	Rig Site 3	807TVR4965
15	Security	Delta 5	Rig Site 4	807TRP860
16	Security	Tiger 1	Mobile Response Unit 1	807TVH4367
11	Security	Tiger 2	Mobile Response Unit 2	871TRPE310
12	Geology	Golf 1	Geo Manager	752TUHA684
13	Geology	Golf 2	Geo Superintendent	752TSN6448
14	Geology	Golf 3		752TRHC653
15	Geology	Golf 4		752TSN5813
16	Geology	Golf 5		752TWKQ154
17	CR	Romeo 1	CR Manager	752TWK0228
18	CR	Romeo 2		752TWK0284
19	CR	Romeo 3		752TYK1561
20	CR	Romeo 4		752TYK2412
21	CR	Romeo 5		752TYK2432
22	Tembo	Tango 1		752TYK3613
23	Tembo	Tango 2		752TYK3906
24	Tembo	Tango 3		752TYK4252
25	Tembo	Tango 4		752TYK4309
26	Tembo	Tango 5		752TYK3854
27	Tembo	Tango 6		752TYK3688
28	Tembo	Tango 7		752TYK4221
29	Tembo	Tango 8		752TYK4454
30	Tembo	Tango 9		752TYK3778
31	Tembo	Tango 10		752TYK3734
32	Tembo	Tango 11		752TYK3646
33	Tembo	Tango 12		752TYK3640
34	Tembo	Tango 13		752TYK2638
35	Tembo	Tango 14		752TYK3762
36	Tembo	Tango 15		752TYK2426

MOTOROLA BASE STATION VHF RADIOS

Radio No	Location	Callsign	SN
1	Control Room	Zero	511TVMA683
2	MRU 1 Vehicle	Tiger 1	TBC
3	MRU 2 Vehicle	Tiger 2	TBC
4	Geo Vehicle	Golf Victor	TBC

VEHICLE SATELLITE TRACKING

Vehicle No	Owner	Make	VRN
1	Tembo	TLC	T387 DTB
2	Tembo	TLC	T859 AUF
3	Tembo	TLC	T755 DUS
4	HAP	TLC	T628 DYB
5	HAP	TLC	T515 EBN
6	HAP	TLC	T517 EBN
7	RSK	Mitzubitshi	T722 DQJ
8	RSK	Mitzubitshi	T440 DQH
9	RSK	Mitzubitshi	T439 DQH
10	RSK	Toyota Hilux	T726 DSE
11	RSK	Toyota Hilux	T724 DQJ
12	RSK	Toyota Hilux	T663DQJ

SATELLITE PHONES

Phone No	Owner	Make	SN
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

14. EMERGENCY CONTACT INFORMATION

14.1 Internal Emergency Contact List

Table 10: Internal Emergency Contact List

Name	Position	Phone Number
TEMBO DAR ES SALAAM OFFICE		
Benedict Busunzu	CEO	+255 754 569 788
Frank Kilua	CFO	+255 767 101 100
Manny Ramos	COO	+255 753 647 564
Saimon Sanga	CHRO	+255 762 779 177
Catherine Metili	Executive Assistant	+255 769 989 004
Bosco Kigodi	Transport Officer	+255 739 446 611
Clever Mrema	IT Manager	+255 767 210 985
Levina Christopher	Senior Officer Administrator	+255 757 000 032
Mariagoreth Charles	Communications Manager	+255 768 660 492
KABANGA SITE		
LEADERSHIP		
Rebecca Stephen	General Manager	+255 759 366 400
Dr Kudra Said Mfaume	OHS&S Manager	+255 759 340 654
Tunzo Msuya	Environment Manager	+255 767 999 992
Basil Shio	RAP Manager	+255 629 800 000
Peter Shemkai	Acting Site Human Resources Manager	+255 767 157 358
Moses Rusasa	Community Relations Manager	+255 757 141 618
Kirmat Noormohamed	Chief Geologist	+255 745 885 341
TNCL SITE SECURITY		
Charles Kisuke	TNCL Site Security Lead	+255 743 134 334
HAP SITE SECURITY		
Security Control Room	24-hour Control Room (emergency)	+255 767 912 555
Duty Shift Commander	24-hour Shift Commander (emergency 2)	+255 767 212 555
Gilles Muroto	Site Security Manager	+255 715 291 944
Elia Mimbi	Deputy Site Security Manager	+255 752 298 912
Jeremiah Romward	Ops and Training Commander	+255 626 933 037
Simon Revelian	Guard Force Commander	+255 752 974 482
TNCL SITE SAFETY		
Dr Fredrick Weinand	Occupational Health Lead	+255 786 652 325
Dr Ikunda Mbise	Medical Doctor	+255 745 660 097
Dr Octavian Byeshurilo	Medical Doctor	+255 745 660 097
Gadiel Kirika/ Diana Ladislaus	Paramedic	+255 745 998 896
Akida Waria	Safety Lead	+255 765 855 817
Riziki Msule	Safety Officer	+255 748 238 357
ERT Emergency Number	24-Hour ERT Number	+255 745 221 995
Habibu Msabila	ERT Coordinator	+255 754 576 956
Fulgence Bizimgabe	Safety and Training Specialist	+255 757 494 585
OTHER SITE DEPARTMENTS		
Michael Mhanuka	Project Lead – Kahama	+255 752 515 753
Naziel Eliakimu	Environmental Lead – Kahama	+255 752 428 046
Florence Nyuki	Environmental Lead	+255 763 000 574

Moses Rusasa	Community Relations Manager	+255 757 141 618
Vivian Otieno	Senior Community Relations Officer	+255 755 577 080
Susanne Mbise	Communications Lead	+255 766 263 844
Fred Azzah	Communications Officer	+255 762 654 614
Jumbe Maulid	Geology Superintendent	+255 754 003 020
Angelrose Mgallah	HR & Admin Specialist	+255 742 610 500
Jacques Marais	Project Superintendent	+255 752 396 160
Johan Blignault	Construction Manager	+255 762 821 825
Joseph Mwita	Training Lead	+255 767 373 496
Azael H. Kitange	Learning and Development Lead	+255 769 219 483
Sarai Ally	Project Superintendent	+255 767 241 288
Omary Hassan	Senior Project Engineer	+255 754907 329
Elinazi Mkilindi	IT Coordinator	+255 744 400 040
Gilman Gration	Travel Office & Camp Driver	+255 765 460 432
Vincent Aloyce	Camp Coordinator	+255 767 403 249
Zamda Japan	Camp administrator	+255 755 831 631
Honest J. Nyombi	AKO Project Manager	+255 752 415 009
Eladius Oisso	AKO SHEQ Officer	+255 748 113 187

14.2 External Emergency Contact List

Table 11: External Emergency Contact List

Name	Position	Contact Number
KAGERA REGION		
Hon. Fatma Mwassa	Regional Commissioner (RC)	+255 713 229 677
SACP Blasius Chatanda	Regional Police Commander (RPC)	+255 717 444 107
SSP Mayala Boniface	Regional Crime Officer (RCO)	+255 714 293 410
SP Peter Mtali	Regional Traffic Officer (RTO)	+255 754 095 127
RFO Muhuma	Regional Fire Officer (RFO)	+255 676 392 399
NGARA DISTRICT		
Col Mathias Kahabi	District Commissioner Ngara	+255 754 509 557
William Solla	OCD Ngara	+255 755 700 871
ASP Kisaka	OC - CID Officer	+255 621 662 429
INSP Kamgisha	OCS Rulenge	+255 746 260 123
A/INSP Kazen	OCS Bugarama	+255 710 460 492
INSP Kalaso	OCS Murusagamba	+255 765 506 884
Lt. Sugwa	OIC Military Base Bugarama	+255 765 727 755
Dr Deogratius Mlandali	District Medical Officer	+255 625 606 758
A/Inspector Edward J Bishanga	District Fire Officer	+255 754 763 723
Hatujuani Lukari	District Assistant Secretary	+255 718 743 054
HOSPITALS		
Hospital Secretary	Rulenge Mission Hospital	+255 620 601 876
Mwanza Hospital	Bugando Government Hospital	+255 754 803 729
Dar es Salaam Hospital	Aga Khan Hospital	+255 222 1151 51
Kenya Hospital	Nairobi Hospital	+254 27 22 160

15. POLICIES AND STANDARDS

15.1 References to Company Policies and Documents

1.1 TNCL Project Security Risk Assessment October 2023

1.2 TNCL Project Threat Assessment September 2023

1.3 TNCL-OHS-POL-0001, Health and Safety Policy

1.4 TNCL-OHS-SOP-0002, Incident and injury reporting and investigation procedure

1.5 TNCL-OHS-SOP-0033, Emergency callout procedure

1.6 TNCL-OHS-PLN-0001, Emergency Crisis Management Plan

1.7 TNCL-OHS-SOP-0039, Medical Emergency Evacuation Procedure

1.8 TNCL-OHS-PLN-0005, Journey Management Plan

1.9 TNCL-CRE-SOP-0001, Grievance Mechanism Procedure

1.10 HAP-TNCL-POL 0001 VPSHR Policy

1.11 TNCL Disciplinary Policy

1.12 TNCL Environmental and Social Impact Assessment

1.13 TNCL and Tanzanian Police Force Memorandum of Understanding (12th May 2023)

15.2 General Reference Documents

1. IFC Good Practice Handbook (2009) Addressing Grievances from Project-Affected Communities.
2. IFC Good Practice Handbook (2017) Use of Security Forces: Assessing and Managing Risks and Impacts.
3. IFC Good Practice Handbook (2009) Addressing Project-Induced In-Migration.
4. IFC Performance Standard 1 (2012) Assessment and Management of Environmental and Social Risks and Impacts.
5. IFC Performance Standard 4 (2012) Community Health, Safety, and Security.
6. ISO 30001 (2018) Risk Management Guidelines.
7. ISO 31030 (2021) Travel Risk Management.
8. ISO 9001 (2015) Quality Management.
9. International Code of Conduct for Private Security Service Providers (2010) Principles and standards applicable to private security companies (companies providing guard forces).

10. UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (1990) Principles on use of force and firearms by law enforcement officials.
11. UN Code of Conduct for Law Enforcement Officials (1979) Principles and prerequisites for law enforcement officials to perform their duties while respecting and protecting human dignity and human rights.
12. UN Guiding Principles on Business and Human Rights (2011) Global standard for preventing and addressing the risk of adverse human rights impacts linked to business activity.
13. Voluntary Principles on Security and Human Rights (2000) Internationally recognized set of principles designed to guide companies in maintaining the safety and security of their operations within an operating framework that encourages respect for human rights.

15.3 Security Standard Operating Procedures

1. TNCL-SEC-SOP-001, SITE ACCESS AND MATERIAL CONTROL
2. TNCL-SEC-SOP-002, KEY CONTROL
3. TNCL-SEC-SOP-003, SECURITY THREAT CLASSIFICATION AND MANAGEMENT
4. TNCL-SEC-SOP-0004, MISSING PERSON PROCEDURE
5. TNCL-SEC-SOP-0005, KIDNAP AND RANSOM PROCEDURE
6. TNCL-SEC-SOP-0006, SECURITY CONTROL ROOM OPERATIONS
7. TNCL-SEC-SOP-0007, SECURITY WORKING GROUP PROCEDURE
8. TNCL-SEC-SOP-0008, WORKING IN ISOLATION PROCEDURE
9. TNCL-SEC-SOP-0009, TNCL AIR OPERATIONS PROCEDURE
10. TNCL-SEC-SOP-0010, BURUNDI NEIGHBOURHOOD SECURITY MEETING
11. TNCL-SEC-SOP-0011, CONFIDENTIAL INFORMANTS
12. TNCL-SEC-PLN-001, SECURITY MANAGEMENT PLAN
13. TNCL-SEC-PLN-0003, NGARA AIRPORT EMERGENCY RESPONSE PLAN
14. TNCL-OHS-SOP-0002, INCIDENT, INJURY REPORTING AND INVESTIGATION
15. TNCL-OHS-SOP-0033, EMERGENCY CALLOUT PROCEDURE

16. SYSTEM EVALUATION

This plan shall be reviewed at least after two years by members of the Security department and presented to the Standard Committee for approval, or when organizational changes take place or required as part of internal and external audits. The TNCL Document Controller will monitor compliance with the document control system on an ongoing basis.

17. DISTRIBUTION

List physical locations which require a controlled copy of this document.

Table 12: Distribution

Copy	Controlled Document Folder Location
Master	Controlled Documents Central Filing System

18. CONTRAVENTION

Any breach of this plan shall be regarded as refusal/failure to carry out a lawful instruction and will be dealt with as per the disciplinary procedure.

19. DOCUMENT CHANGE PROCESS

The process of document change starts when the document custodian identifies there is a need to make changes within the document. The document custodian/ owner shall complete the document change request form, sign it off and submit it to the Document Controller.

The Document controller shall issue the controlled word copy of the document to the respective document custodian/owner so that changes may be made. The document custodian/owner shall resubmit the updated document to the document controller so that the document can be controlled and updated within the Filing system ready for use by the end users.

19.1 Reason for Change

Table 13: Reason for Change

A	As a result of incidents	F	Change in training requirements
B	As a result of the audit findings	G	Results of risk assessments
C	New / changes in governance documents	H	Change due to spelling or grammatical error
D	Changes in legislation	I	New document format
E	Changes in technology	J	To integrate special instruction into the document control system

19.2 History of Change

Table 14: History of Change

Date of Change	Revision No	Revised Item (paragraph Number reference if required)	Reason Code	Name of Reviewer

20. RECORD CONTROL

Table 15: Record Control

Document Title:	Document ID:	Responsible for Maintenance:	Responsible for Filling:	Location of Storage:	Retention Period:	Method of Disposal:
Security Management Plan	TNCL-SEC-PLN-0001	Document Controller	Document Controller	OHS Department	Hard Copy two Years	Hard copy shared file electronic

21. DECLARATION

I hereby declare that I have taken part in the discussion of this plan, and I understand its contents and do commit that I shall ensure compliance hereto:

	Name and Surname	Company Number	Designation / Role	Signature	Date Signed
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					