SECURITY MANAGEMENT PLAN

For:	Transnet Port Terminals (TPT), Saldanha
Project Name:	FEL3 - Saldanha Bulk Terminal Equipment Refit: Stacker Reclaimers, Ship Loaders and Tippler 2. (Phase-4: Stacker Reclaimer 3)
Project Number:	Z.5200160

Author:	Marlene Nel
Owner:	Louis du Toit (Terminal Manager)
Client:	Transnet Port Terminals (TPT)
Project Sponsor:	Andiswa Dlanga(Managing Executive)
Project Manager:	Graham Handley

Revision Number:	00
Approved by:	Ntsikelelo Nteta
Document No:	Z.5200160-SMP

DOCUMENTATION DISTRIBUTION, REVISION AND APPROVAL HISTORY

REVISION NUMBER	DATE	DISTRIBUTION	PREPARED BY	REVIEWED BY	APPROVED BY
00	12/01/2021	1	M. Nel	G. Handley	N. Nteta

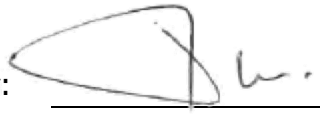
SIGNATORIES:

Prepared by:  18.01.2021

Marlene Nel
Terminal Security Manager
Date

Reviewed by:  19/01/2021

Graham Handley
Snr. Project Manager
Date

Approved by:  19/01/21

Ntsikelelo Nteta
Regional Risk & Compliance Manager
Date

TABLE OF CONTENTS

Section 1 Administrative details

1.1 Authority

This Security Plan was compiled by Graham Handley, and was reviewed by Security Manager, Marlene Nel. The Security Department supports the implementation of the plan. The plan is submitted for approval by the relevant Program members.

Section 2

Scope

Refer to Annexure 1 – Baseline Security Risk Assessment, which was conducted and serves as input to this document.

The scope of this security management plan is to identify and prioritise the various security risks involved with a project of this magnitude. Secondly a cost-effective solution must be agreed upon by all Project members involved. This document to be read with all attachments.

Project Managers may wish to expand the coverage of their plan to include related operations and activities.

All aspects of security are covered in the plan. These include but are not limited to:

Security administration

Physical security

Mobile security

Personnel security

Asset security

Standard operating procedures, rules and requirements are listed in Annexures 2, 4, 5, 7 and 8, and should be read in conjunction with this document.

Section 3

Project Overview

Project Manager	Graham Handley	
Construction Manager	To be appointed	
Safety Practitioner	Rejean Viljoen	
Security Manager	Marlene Nel	

3.1 Operational Plan Layout

3.2 Physical Security Layout

Post	No. and Grade of officer	Day Shift	Night Shift	Post specific Equipment
Access Control	Grade C			Shelter Portable Toilet Handheld radio PPE Torch Occurrence Book Access control register Breathalyser
Supervisor	Grade B			Shelter Portable Toilet Handheld radio PPE Torch Occurrence Book Access control register Breathalyser

Section 4 Consultation, Communication and Coordination

4.1 **Security plan mechanism for consultation*:***

a) Between the Project Team and members of the TPT Security Department.

b) Between TPT Security Department, local SAPS and TNPA security.

c) Between TPT Security Department and its personnel and contractors regarding security measures and procedures to be implemented.

4.2 **Stakeholders communication and consultation:**

A monthly steerco Meeting will be held with stakeholders from TNPA, TPT, BTS, Mines etc, as well as senior management representatives of the project. Security will be discussed at these meetings as well as at the weekly project meetings. For further information regarding identified stakeholders refer to stakeholders listed in the Project Execution Plan, Z.5200160-PEP.

4.3 **Employees and contractors:**

Employees and sub-contractors will need to assist with the implementation of security measures and procedures on site, as well as reporting of any incidents per flash report to Security timeously.

Section 5 Operation of the Plan

5.1 Review and audit

- TPT Security will ensure that the plan is effective and adequate and that the plan has been implemented correctly by means of a monthly site audit by TPT in house security staff when applicable.
- This will include a consultation with employees and project managers to ensure security measures and procedures are adequate and the plan is appropriately implemented.
- It is suggested that for ease of maintaining audit and review procedures that they should be referenced in this section and specific details included as attachments.
- Penalties can be implemented as per Transnet's Master Service Level Agreement, Low to High risk area.

5.2 Responsibilities

The Project Security Plan must detail the specific duties and responsibilities of the Security Manager and other security personnel (for example the duties and responsibilities of any security officers employed or contracted to TPT for the projects).

Position	Responsibilities
Security Manager	Conduct audits per project site Liaise with security companies Report on findings to project managers
Senior Investigator	Investigate any incidents and review site instructions Assist with site audits Implement changes needed to site security
Outsource Contract Security Officers	Patrol of site premises and access control Record all incidents/ irregularities in site occurrence book Report to control room and TPT & TNPA Security.
Security Control Room Operators	Manage daily site postings Report any irregularities to TPT Security Manager Be in constant contact with sites under their control

5.3 Knowledge and training

Transnet must ensure that security guards with responsibility for security have adequate knowledge and have received appropriate training to be able to carry out their duties. If findings find a lack of knowledge regarding executing his/her security function refresher training must be immediately implemented. This includes site security specific, safety training, referred to as site induction. On the job training should be done by service provider.

PSIRA will also be confirmed per security guard and companies will be required to always wear appropriate PPE on all project sites. Any guard found/seen on site without the correct PPE will be removed and replaced at the contractor/security companies own cost.

Security File per site must be provided and include:

- List of training or qualifications per guard:
- PSIRA certificate. (SAPS certified)
- CV and course certificates
- Identity Documents (SAPS certified)
- All relevant site induction material pertaining to specific site
- First Aid
- Fire Fighting
- Standard Operating Procedures site specific.
- Company Security Officers site instruction and work procedures
- Company site contingency plan/strike plan.
- Security disciplinary code for security officers.
- Detailed contact list in case of emergency displayed

Monthly security performance review will be conducted on file.

5.4 Project Security Induction:

Project security supervisor name, security office and contact details

Security Policy

Crime trends and hotspots (refer to annexure 6 for Security Statistics)

Project weapons, cameras, drug and alcohol policy (refer to annexure 8 for procedure for photography control)

Access badge and Identification

Response to facility security incidents

Classification of suspicious activity and how to report it

Section 6 Security Measure and Procedures

6.1 Security measures and procedures.

All measures and procedures per site will be attached at the end of the document and labelled accordingly, referred to as Standard Operating Procedures (SOP). Refer to the following annexures: Annexures 2, 4, 5, 7 and 8.

a) Measures to prevent unauthorised carriage or possession of weapons or prohibited items on the site;

If appropriate, these measures could include but are not limited to:

- The screening and clearing of staff and visitors when accessing the site.
- Following of Transnet fire-arm policy and Access Control policy (Annexure 7 – Port Access Control Standard Operating Procedure).

b) Measures to prevent unauthorised access to the site ;

If appropriate, these measures could include but are not limited to:

- Perimeter fencing around the site boundaries covered by the plan;
- Procedures for the clearing of people that wish to enter the project site;
- Regular security patrols;
- List of authorised project staff for access control measures.

c) Procedures for responding to security threats or breaches, including provisions for maintaining critical operations on the site;

If appropriate, these procedures could include but are not limited to:

- Procedures for armed response to respond to level 1 situation.
- Procedures for the contacting of National Command Centre as well as Group Security if threat warrants it. Level 2 and above

d) Procedures for responding to and implementing any new security standards or legislation issued or initiated by Transnet Group;

If appropriate, these procedures could include but are not limited to:

- Management procedures that will be taken to ensure that a new security standard or legislation is implemented as soon as possible after being issued.
- Procedures for communicating the new procedures within Transnet and externally where necessary.

e) Procedures for evacuation of the site in case of security/safety threats*;*

This should include reference to a current contingency/evacuation plan*.*

f) Procedures for reporting occurrences (e.g. security breaches) which threaten the security of the site;

These procedures should include, but are not limited to, procedures for reporting occurrences to:

- National Command Centre;
- the SAPS;
- Internal procedures (flash reports) for employees to report security breaches/incidents to management or the Security Manager.
- Procedures for raising the awareness of staff of their responsibilities for reporting incidents.

g) Measures to ensure the security of physical assets of Transnet at the site;

The security plan will include measures to protect the physical assets of the institution at facilities of the institution.

If appropriate, these procedures could include but are not limited to:

- Requirements for admission/receiving of material or supplies.(TNPA port entrance to declare all equipment entering the port)
- Controls for movement of assets on the premises from one area to another. (Material registers/Material despatch register)
- Permission slips (three fold) for removing assets of Transnet from the site.
- Material Movement - SAP 16 Process Flow. (Annexure 3)

6.2 Security Level 1

These measures must include:

- The security measures identified in the security TRA for the institution, for implementation at Security Level 1.

This table can be used to record the security measures.

SECURITY MEASURES AND PROCEDURES AT SECURITY LEVEL 1

Description of security measure or procedure.	**Person with responsibility for implementing the measure or procedure**
Perimeter Fencing, staff security clearances, security guard patrols etc.	Security Manager, Security Officials Employees, etc.

6.3 Security Levels 2 and 3

The following tables can be used to record the security measures and procedures.

SECURITY MEASURES AND PROCEDURES AT SECURITY LEVEL 2

Description of security measure or procedure.	Person or Organisation with responsibility for implementing the measure or procedure
Increased number of security guard patrols, limit access to site for non-essential personnel.	Security Manager, Security Officials, Employees, etc.

Note. Security Level 2 measures or procedures are in addition to all of the measures and procedures in force at security level 1.

SECURITY MEASURES AND PROCEDURES AT SECURITY LEVEL 3

Description of security measure or procedure.	Person or Organisation with Responsibility for implementing the measure or procedure
Evacuation of site where threat has been identified.	Security Manager, Security Officials, Employees, etc.

Note. Security Level 3 measures or procedures are in addition to all of the measures and procedures in force at security levels 1 and 2.

IMPLEMENTATION TIMETABLE

Security Measure or Procedures	Status (Operational / To be established)	Date of expected implementation (if status is to be established)	Interim measures / procedures
Perimeter security fencing.	To be established	Fencing to be in place by completion of site establishment	Temporary barriers and signs installed to identify the construction area. Additional guard patrols to monitor and deter any

			unauthorised access.
Flash report	Reporting line followed	Directly after incident has taken place.	Notify security of the incident and complete the incident Flash report documentation.

Section 7

Communication

Communication is vital for the routine day to day administration of the function, as well as ensuring that all vested parties are notified of security matters in a timeously manner, facilitating the initiation and implementation of an appropriate response, to events that could impact the security and safety of personnel.

A single point for reporting of security related information will be maintained by the security manager or appointed representative. The security representative is responsible for the verification of all information.

Relevant security information is to be cleared by program manager for release and distributed as soon as possible via email or mobile phone messaging.

Security Communication can be classified as follows:

- Routine security communications
- Security flash notifications
- Security Incident reporting

Section 8

Security plan and review

This plan needs to be reviewed in response to any security incident that highlights deficiencies that's needs to be address.

Annexure 1: Baseline Security Risk Assessment

Annexure 2: Standard Operating Procedures: Security Company, Contractor & TPT

Annexure 3: SAP 16 Process flow

Annexure 4: Minimum Physical Security Standards

Annexure 5: Port Rules

Annexure 6: Security Statistics

Annexure 7: Port Access Control Standard Operating Procedure

Annexure 8: Procedure for filming and photography control