

SERVICE LEVEL AGREEMENT ("SLA")

in respect of the provision of

SECURITY SERVICES

entered into by and between

TRANSNET SOC LIMITED Ltd

Registration Number 1990/000900/30

A public company with limited liability and duly incorporated
in compliance with the company laws of the Republic of South Africa

Operating as

Transnet Property

Registration number 1990/000900/30 –

96 Rissik street

Johannesburg

4001

(hereinafter referred to as the "TP")

and

The Service Provider

Registration Number

(hereinafter referred to as the "Service Provider")

Service Level Agreement for the provision of security services at various sites (hereinafter referred to as "the security services") for Transnet SOC Limited (registration number 1990/000900/30) trading as Transnet Property (hereinafter referred to as "TP") for a period of twelve (12) months

SERVICE LEVEL AGREEMENT ("SLA")

FOR THE PROVISION OF SECURITY SERVICES AT VARIOUS TERMINALS AND SITES (HEREINAFTER REFERRED TO AS "THE SECURITY SERVICES") FOR TRANSNET SOC LIMITED (Registration Number 1990/000900/30) TRADING AS TRANSNET PROPERTY (HEREINAFTER REFERRED TO AS "TP") FOR A PERIOD OF TWELVE (12) MONTHS

By:

Tender Reference:

1. Parties to the SLA

1.1 The Service Level Agreement will be executed by and between TP regions; Inland, KZN , Northern , Western and Eastern Cape and the Service Provider.

2. Purpose

2.1 The purpose of the Service Level Agreement is to define the Security Services offered by the Service Provider and the Security Services required by TP (applicable to both parties) and to quantify these Security Services, where possible.

2.2 This Service Level Agreement also defines the special conditions that will apply for the duration of the Agreement, if any.

3. Scope

3.1 The Master Agreement indicates the Effective Date of the Security Service and the Security Service shall continue to operate until the Termination Date that being (termination date) as stated in the Master Agreement, unless terminated by the TP in terms of Clause 26 of the Master Services Agreement.

3.2 The scope of the Security Services provided by the Service Provider is summarized as to provide an effective, efficient and professional Security Service to TP whereby:

- The TP's assets, plant, equipment, infrastructure and people, including information, are safeguarded;
- TP Customers are safeguarded;
- Identify, assess, report and react to security risks, threats and vulnerability to prevent such incidents from happening;
- Full compliance to all related Transnet / TP Security Strategy, Policy, Standard Operating Procedures and Job Descriptions/Work Instructions; and
- Adequate communication and written reporting on all matters of security.

3.3 Note that an additional description of work (Security Services) that is site-specific is included as per:

- Annexure "A" – Works document (Resources required as per Pricing schedule)
- Annexure "B" – Job Descriptions/Work Instructions per site/deployment area

Service Level Agreement for the provision of security services at various sites (hereinafter referred to as "the security services") for Transnet SOC Limited (registration number 1990/000900/30) trading as Transnet Property (hereinafter referred to as "TP") for a period of twelve (12) months

4. Responsibilities

4.1 TP must ensure that the implementation of adherence to and dissemination of the provisions of this Agreement are clearly articulated to the Service Provider. This is observed through the following:

- Signed Master Agreement between TP and the Service Provider
- Signed SLA between TP and the Service Provider (this document)
- Service Provider Management Induction Programme
- Additional Induction Programs at all relevant TP Sites, including safety induction

4.2 The Service Provider must ensure a clear understanding of its obligation in terms of the SLA and that the necessary care and diligence is continuously exercised in fulfilling its duties in terms of the Master Agreement and the SLA.

5. Training

5.1 Further to paragraph 12.2 of the Master Services Agreement, the following training requirements apply:

- A SASSETA qualification equal to the PSIRA training certificate for a specific grade will also be accepted.
- Dog Handler
- Firearm competency
- Drivers license
- And all other competencies required as per applicable legislations as dictated by standard operating procedures.

6. Communication Forums

6.1 Authorized officers and members of the Service Provider and TP must attend scheduled and emergency communication forums.

6.2 The following are key contact persons:

- Security Manager/ Supervisor & Contact number(s)

6.3 The following are key contact persons:

- Area/Site Manager & Contact number(s)
- Site Inspector & Contact number(s)

6.4 The following minimum communication forums apply:

- Monthly Meetings will be held on the last Wednesday of every month between 12H00 and 14H00.
- Weekly, Ad hoc and or Emergency Meetings
The venue for the above meetings will be confirmed prior to the meeting.

6.5 The following items will form part of every Agenda for the weekly and monthly meetings:

Welcome

1. Present & Apologies
2. Confirmation of Previous Minutes
3. Matters Tabled For Discussion
4. Matters Arising
5. Standing items for discussion
 - 5.1 Security Incidents – reports, corrective action, etc.
 - 5.2 Disruptive Operations planning
6. Contract Management
 - 6.1 Officer files update
 - 6.2 Penalties sign off
 - 6.3 Performance Balance Scorecard sign off (monthly meeting only)
 - 6.4 Other (e.g. Claims, Training, Safety inductions, Medicals, etc)
7. Emerging Security Risks Identified and Action Plans
8. Occupational Health and Safety minutes – items for action (monthly meeting only)
9. New Matters
10. Conclusion

7. Equipment

The following equipment need to be supplied by the Service Provider for use in the Region by the officers:

7.1 All equipment as listed in clause 11 of the Master Service Agreement

7.2 All Region specific Personal Protective Equipment (PPE) is required:

- 7.2.1 The list of the specific PPE requirements for each terminal is listed on the "Scope of Work" document attached as Schedule 1 to the Master Agreement
- 7.2.2 In the event of any national or global health scare such as the Covid-19 pandemic in 2020, the service provider will bear the cost for any prescribed PPE to be worn to protect its employees deployed on the frontline. This PPE will be supplied by the service provider to its employees until such time that the South African Department of Health has declared it no longer necessary.

7.3 The following facilities/equipment on TP asset register is provided to **XXXX** for use during the contract period as per the MASTER AGREEMENT:

- Guard Houses (Permanents and Temporary)
- Toilets
- Lockers
- Tables
- Chairs
- Kettle
- Microwaves
- Cleaning Material (i.e. brooms, mops, soap etc.)
- Communication devices
- Alcohol testing devices
- Any other additional/innovative equipment required to be utilised in TP.

Complete a separate "handing over" certificate which lists all existing damages and on which the service provider's delegated authority sign for receipt of the equipment/facilities.

TP's assets supplied to the Service Provider for the execution of their duties remains the property of TP and will at any time be available for inspection by TP Security representative. Any such assets in the possession of the service provider, on completion of the agreement must be returned to TP in the same working condition as handed to the Service Provider.

The Service Provider will be responsible for any loss or damage to TP assets issued for use during the contract period. If required TP will deduct the loss/damage of such equipment/asset from the invoice, if the service provider fails to compensate TP.

8. Ad Hoc and Emergency services

- 8.1 TP will have control and monitor processes to procure ad hoc and/or emergency services.
- 8.2 Ad hoc and/or emergency services are determined within the discretion of TP depending on the circumstances and the required type of special security arrangements. These requirements will be formally communicated to the Service Provider as prescribed in paragraph 4.6,5.6,5.7 and 12.7 of the Master Service Agreement .
- 8.3 Ad hoc and/or emergency services will be utilized as requested by TP and maybe of a temporary nature.
- 8.4 Annexure "C" – Service Request Form, will be used as documentary proof for the sourcing of ad-hoc and/or emergency services. All telephonic requests by TP authorized personnel for these services will be followed up in writing within 4 hours of the request. Should the cause of the emergency prevent this, the request must be appended in writing, as soon as possible and within reasonable time limits.
- 8.5 The services will be paid for as per agreed price structure in the Master Agreement.
- 8.6 The Service Provider must adhere to the start and end date listed on the Service Request Form for ad hoc services.

9. Performance measurements

- 9.1 TP has a monthly performance measurement tool for specific Security Services provided and is attached as: Annexure "D" – SLA Performance Balance Scorecard

The following performance indicators are relevant:

For scores out of 5:

- 1 = Unacceptable,**
- 2 = Below standard,**
- 3 = Acceptable &**
- 4 = Consistently exceeding TP expectations**

Service Level Agreement for the provision of security services at various sites (hereinafter referred to as "the security services") for Transnet SOC Limited (registration number 1990/000900/30) trading as Transnet Property (hereinafter referred to as "TP") for a period of twelve (12) months

9.2 Notwithstanding the terms & conditions contained in the Master Agreement, the following areas will form part of the SLA Performance Balance Scorecard:

- a) Management of Capacity
 - i. Planning
 - ii. Security operations
- b) Legislative Compliance
 - i. Safety and Security Requirements
- c) Invoicing and Payments
- d) Penalties
- e) Claims
- f) Non-conformances
- g) Continuous Improvement

9.3 The information will be conveyed monthly to the office of the TP Regional Security Supervisor for the monitoring of service levels and if it is still to the expectation of TP.

In the event of an unplanned and illegal strike of the work force of the Service Provider, TP will invoke the provisions as listed under clause 25.13.

10. Incident reporting

10.1 Records of incidents and transgressions across Regions must be reported not later than at the end of the shift to the TP Security representative on duty.

10.2 Serious incidents or incidents of a criminal nature that may attract media coverage must be reported immediately to the TP Security representative.

10.3 The incident report should contain the following information.

- Date and time of incident
- Nature of incident.
- Place of incident.
- Injuries and lossess suffered, approximate value of the loss
- Description of incident.
- SAPS case number if applicable.
- Arrest made and name of suspects.
- Name of person who reported the incident.
- Preliminary findings.
- Name of investigator.

11. Penalties

Penalties for non-conformance will be raised as per clause 20 in the Master Agreement.**Error! Reference source not found.** In terms of clause 20 the following ratings will apply to the TP sites: – Risk rating of all TP facilities is "High, medium and low".

12. Contingency Plan and Risk Assessment

12.1 A Security Risk Assessment, using a recognized risk management methodology, must be conducted regularly (at least once a quarter) in collaboration with the TP Security Supervisor to ensure that security measures are aligned to the security risks and threats. The risk

Service Level Agreement for the provision of security services at various sites (hereinafter referred to as "the security services") for Transnet SOC Limited (registration number 1990/000900/30) trading as Transnet Property (hereinafter referred to as "TP") for a period of twelve (12) months

assessment must also indicate the recommendations to mitigate the identified risks and threats.

12.2 TP has business continuity, contingency and emergency response plans to cater for the following:

- Major business interruptions
- Emergency events (Safety and Security incidents)
- Labour/Protest action

12.3 Accordingly, the Service Provider will provide TP with their contingency arrangements and ensure that the data provided to TP remains current.

12.4 The Service Provider will formally report any 'new' or emerging risk(s) or security threat(s) to the TP Security Supervisor immediately when they observe and/or gain knowledge thereof.

12.5 It is expected that the Service Provider will also draft contingency plans for the effective continuation of service when required by the TP. Examples of events that require contingency plans are:

- Major events hosted by Transnet or Government that may have an impact on security operations within the TP;
- December festive period;
- Easter holidays;
- Vehicle breakdowns
- Own Staff Labour Unrests/Strikes
- Absenteeism

13. Job Descriptions

13.1 TP will provide job descriptions/Work Instructions/Standard Operating Procedures for all premises and areas under its control.

14. Review

14.1 Performance levels against the SLA will be reviewed quarterly. The monthly Performance Balance Scorecard will be used as source document for the quarterly review and to track improvements or declines in the Security Service.

15. Request for Change

15.1 All changes to the Work Document as stipulated in Annexure "A" will be affected by TP, using the Security Change Request Form – see Annexure "C" of this Service Level Agreement.

15.2 All approved changes to be communicated in writing to the Service Provider by the TP Security Manager.

16. Removal of officers

16.1 If the actions or performance of an officer is to the detriment of TP or creates a risk exposure, the immediate removal of such officer will be requested telephonically by the TP Security

Service Level Agreement for the provision of security services at various sites (hereinafter referred to as "the security services") for Transnet SOC Limited (registration number 1990/000900/30) trading as Transnet Property (hereinafter referred to as "TP") for a period of twelve (12) months

Manager or his/her appointed as per Annexure G and as per clause 25.13 of the MSA. An email from TP to the Service provider will follow thereafter.

16.2 An officer removed from a TP site will not be re-deployed onto another Transnet site without the written consent of the Security Manager where the person will be re-deployed.

16.3 In the event that security officers are suspected of involvement in any criminal activity, they must be subjected to a polygraph test or screening by an independent service provider, at the cost of security service provider. The security service provider cannot conduct its own polygraph tests or screening, even if it does have this capability available in-house.

Signed at _____ on this _____ day of _____ 20__

WITNESSES:

Service Provider:

- 1.
- 2.

NAME AND DESIGNATION OF SIGNATORY
WHO WARRANTS THAT HE IS DULY
AUTHORISED THERETO

Signed at _____ on this _____ day of _____ 20__

WITNESSES:

TP – Region:

- 1.
- 2.

Name
Security Manager/ Supervisor

Transnet Property– Security Resource Requirement Region

Location	Security Grade	Hours of Duty	Days per week	Officer per shift Day Night		Duties	Equipment				
		REFER TO SCHEDULE 1 OF THE MASTER SERVICE AGREEMENT ("SCOPE OF WORK")									

XX Day Shift
XX Night Shift
Total Contract Security Guards = XX

Annexure B – Job Descriptions

1. Roles & Responsibilities: Supervising Inspector

Notwithstanding the terms and conditions of the MASTER AGREEMENT the Supervising Inspector:

- must at all times protect the interests of TP to the best of his/her ability, in accordance with the laws and with due regard to the interest of all other interested parties.
- shall ensure that the employees deployed at TP are trained to render the Security Services, are provided with the correct equipment to render the Security Services and are trained to use the equipment effectively.
- shall carry out a minimum of two site inspections per shift
- must assess vulnerability, identify security risks, evaluate controls and recommend immediate steps if a threat is identified
- must make an entry of his/her visit in the occurrence book (OB) on each visit, stating the time and details of any observations.
- is required to maintain a close liaison with the TP Security Department and report any emergency or immediate threat to the TP Security Supervisor on duty.
- will issue an incident report to TP Security Department on any security breaches which occurred within their area of control not later than the end of the working shift within which the incident occurred.

2. Roles and Responsibilities of the Security Officers

- Every security officer that is deployed to render the Security Service to TP must be reliable, fully and correctly informed his/her employer of the level of training, skill, experience and qualifications that he/she has attained and is properly trained and able to effectively use the equipment that he/she is issued with to render the required Security Service to TP.

(a) Access Control – Administrative buildings

The security officer will enforce access control as follows:

TP Staff

- All TP staff will be in possession and display or produce a TP ID card with a clear photo before entry to the building.
- All staff shall use their own security access cards to gain entry through electronic doors.
- Staff who have no ID card or access disk must fill in the visitors register.
- All staff that enters the building after hours, weekends or public holidays must report at security who will note the visit in the OB.
- Staff not in possession of a permanent authority for equipment issued to them, must be in possession of a letter of authorization to remove equipment from the building. This refers specifically to laptop computers and other electronic equipment. The letter of authorization must include the following:
 - Type of equipment (*e.g. Toshiba Pocket PC e350*),
 - Model Number (*e.g. PSA50 YXT*),
 - Serial Number (*e.g. 12345678G*),
 - Issued to - (*Full Name, Department, Phone, ID Number, Signature*)

- Authorised by – (*Full Name, Department, Phone, Signature*)
 - Authorisation period
 - Date
- A copy of the letter of authorization for all staff that have authorization to be in possession of electronic equipment must be available on file at the security desk for control purposes

Visitors & Contractors / Service Providers

- All visitors must show a valid photo ID and sign the visitors register prior to entry
- All visitors will declare their laptops and record the details in the relevant space in the visitor's register, the machine type (*e.g. Toshiba Pocket PC e350*) and Serial Number (*e.g. 12345678G*)
- When visitors leave the building with electronic equipment the recorded details must be compared with the declared items and the security officer will sign the equipment out.
- When visitors exit the building with electronic equipment that was not previously recorded, such details must be recorded in the Register together with a copy of an authorization letter by the relevant Head of Department or Designate. Only then will the security officer sign the equipment out.
- Upon arrival scheduled / pre-authorized Visitors must declare their business and security/reception will phone the host who will meet the visitor at security/reception and escort them to the area of business within the building. Visitors must be escorted back to security upon completion of their business.
- Visitors must not be allowed to remove any TP property without proper written authority.
- All unofficial / unscheduled visitors shall only be allowed access to a designated area when they are met by an authorized escort from the security reception area.
- All visitors carrying packages and baggage must declare the contents. Where X-Ray machines are in use, this packages/baggage must be scanned.
- The same procedures apply for the control of cleaning personnel who enter buildings after normal working hours

(b) Access Control – Operations area

The security officer will enforce access control to all persons who require access to the operational areas of TP as follows:

- At all other TP the procedures for access to the administrative offices applies with the following additional requirements:
 - Security officer ensures that person complies with TP Conditions of Entry and that PPE is available and worn.
 - TP representative from the relevant department is called to confirm appointment.
 - TP representative must collect the visitor and the point of entrance.
 - Person completes access control register and visitors permit/card is issued.
 - After business is complete the person must proceed to the exit point.
 - Security officer verifies that no unauthorized items are removed from site.
 - Security officer collects visitors permit/cards and release person to exit the area.

(c) Deliveries into the operational area

- The delivery company representative presents her/himself to the security officer at the access gate to the operational area.
- Security will not allowed to collect to sign or colect any deliveries.
- The person who receives the delivery will need to collect the delivery and sign for it personally.
- Security officer informs the relevant department telephonically of the delivery and requests a representative to receive the delivery at the relevant delivery point.

(d) Security officer verifies the request for entry through perusal of the delivery note, order form or other form of authority to enter terminal;

- Security officer verifies credentials of vehicle and occupants to ensure vehicle and occupants are accredited as required by TP Conditions of Entry;
- Security officer captures visit in relevant register, searches vehicle if required, ensures occupants have the necessary PPE and allow access to terminal;
- Upon exit from the Property the security officer will perform the necessary searches, document control, if required and capture the exit in the relevant register and allow vehicle and occupants to leave.

(e) Delivery of Cargo

The following procedure will be followed for vehicles delivering cargo to the operational area of the terminal:

- Security verifies the request for entry through perusal of delivery note, booking order form or other form of authority to enter terminal;
- Security officer verifies credentials of vehicle and occupants to ensure vehicle and occupants are accredited as required by TP Conditions of Entry;
- Upon exit from the Property the security officer will ensure that exit is captured by security, if applicable, perform the necessary searches and capture the exit in the relevant register and allow vehicle and occupants to leave.

(f) Communications

- An Instruction Register shall be maintained as a means of communicating concise instructions or information to Service Providers personnel originating from the TP Security department
- Security Officers shall have the ability to communicate quickly and effectively and to operate all communication equipment efficiently
- Security Officers must be competent in after hour and emergency communications procedures and the correct radio procedures.

- Emergency numbers must be clearly displayed in the security reception area and the Security Officer must be aware of the current emergency / duress code to be used when reporting a volatile situation, including reports to SAPS or Security Control Rooms.

(g) Deliveries & Mail

- Security officers must be able to identify or recognize letters and parcels that may contain hazardous substances or explosives
- All deliveries / collections must be scheduled in advance by department heads
- Security officers must receive prior notification of such delivery / collection details (who, what, when, how)
- Upon receiving / collection of goods or equipment, Security officer will compare that to a corresponding pre-schedule entry
- All deliveries / collection must have valid documentation
- Under no circumstances will security officers accept deliveries / collection without supporting documentation
- No deliveries / collection must be kept in the security area without the accompanying documentation; the security officer shall inform the relevant department of any delivery received
- All courier packages must be checked and identified at reception in the courier' presence prior to accepting such packages.
- Housekeeping must be maintained at all times

(h) Video surveillance & Intruder Detection Systems (where required by TP)

- The security officer will monitor the video surveillance cameras and record and report any suspicious incident immediately to his supervisor or TP Security Management.
- Special attention must be given to security high risk areas, i.e. **insert areas**
- Any incident must be recorded onto DVD/mass storage device for future record purposes and must be provided to the TP Security Manager for safe keeping and further disposal.
- An intruder detection system / alarm register must be maintained at properties where this is not integrated into the CCTV system, to record the following:
 - All activations and the reasons
 - Action taken and result
 - Arrests made (provide details of suspect)
 - SAPS case number
 - All maintenance calls and/or services
 - All test activations
 - All Notification of faults or requests to the alarm response company.

(i) Employee parking (where applicable)

- The security officer shall monitor all parking around the building;
- The security officer will ensure that TP staff / Visitors obey the traffic rules within the area;
- The security officer will immediately report any suspicious vehicles or activities to his/her Supervising Inspector;
- The security officer will not allow vehicles to be parked in areas not demarcated for this purpose;

- In all emergencies, the security officer will direct and assist emergency response vehicles.

Code of Conduct for Security Officials

- The Security officer / Supervising Inspector shall not act in matters involving conflict of interest without appropriate disclosures and approval.
- He / She shall truthfully give details of the service he / she can render
- The Security officer shall at all time display honesty and integrity in the performance of his duties.
- The Security officer / Supervising Inspector shall not act in any matters involving conflict of interest without appropriate disclosures and approval.
- The Security officer / Supervising Inspector shall, as far as possible, in the course of rendering the security service to TP comply with all applicable laws, endeavor to protect life and property and prevent crime, with the minimum use of force.
- The Security officer / Supervising Inspector shall safeguard information entrusted to him.
- A Security officer / Supervising Inspector shall not disclose any information originating from a person without written authority of that person
- A Security officer / Supervising Inspector shall not maliciously injure the reputation of his colleagues, TPs or employees.

Annexure "C" - Security Change Request Form

TP	SECURITY CHANGE REQUEST FORM			Reference Number:
DETAILS OF SERVICE LEVEL AGREEMENT TO BE CHANGED				
DOCUMENT REFERENCE	TP TERMINAL NAME	SLA VERSION		
<u>JUSTIFICATION FOR CHANGE (must address security risk and associated costs, budget availability):</u>				
	NAME	SIGNATURE	DATE	DESIGNATION
REQUESTED BY				TP Shift Supervisor
SUPPORTED BY				Terminal Security Manager
APPROVED BY				Terminal Manager/Delegated Authority

Annexure D – SLA Performance Balance Scorecard

Notes on Implementation

- Non-Compliance will not be tolerated
- Monitoring: Bi-monthly performance reviews with TP management and the Service provider.
- Reporting: Bi-monthly SLA compliance reports submitted to TP management by the Service provider.
- Corrective Action: Any breach triggers deductions, contract review, immediate remedial training or redeployment.
- Escalation: Repeated non-compliance and any major breaches will lead to contract termination

Performance	Key performance Indicator	Key performance target	Penalties
Statutory inspection compliance	Inspections of sites in line with requirements of the contract	100%	<ol style="list-style-type: none"> 1. Fifteen (15%) of monthly invoice (evaluated Bi-monthly) payable the next month. 2. Two (2) Consecutive non-conformance will result in termination of contract inline with the MSA breach clause
Reduction in security incidents	Reduction of security incidents Bi-monthly (every second month)	50%	<ol style="list-style-type: none"> 1. Fifteen (15%) of monthly invoice (evaluated Bi-monthly) payable the next month. 2. Consecutive non-conformance in a period of two (2) months will result in termination of contract inline with the MSA breach clause.
Statutory compliance to the minimum PSIRA illustrative wage	Compliance with minimum wage	100%	Non compliance will result to termination of contract inline with the MSA breach clause.
Safety	Life threatening incidents	<0%	Non compliance will result to termination of contract inline with the MSA breach clause.
Skills based and compliment staff	As per skills in the pricing data scope of work	100%	<ol style="list-style-type: none"> 1. Deduction for skill not found - 20% deduction for each guard from the respective site monthly invoice. 2. Consecutive non-conformance in a period of two (2) months will result in termination of contract inline with the MSA breach clause.
PSIRA contraventions	% compliance with PSIRA regulations. Number of notices issued	100%	<ol style="list-style-type: none"> 1. 15% of the monthly invoice, amount payable the following month. 2. Consecutive non-conformance in a period of two (2) months will result in termination of contract inline with the MSA breach clause.

	NAME	SIGNATURE	DATE	DESIGNATION
Rating achieved:	Accepted/not accepted			
Signed by				TP Security Supervisor
Accepted By				Security Service provider
Acknowledged				Security Service Provider

Annexure E – Incident Report

SECURITY OCCURRENCE TECHNICAL FORM

1. Date of Occurrence : _____

2. Time : _____

3. Occurrence Book Reference No. : _____

4. Occurrence Ref. No. : _____

5. Type of Security Occurrence (See List) : _____

6. Committed by who

- Transnet employee
- Transnet contractor Specify _____
- External Specify _____
- Un-identified

7. Name of Transnet employee : _____

8. SAP Number : _____

9. Nature of employment : _____

- a. Permanent
- b. Contract
- c. Trainee

10. In case of Theft, what kind of theft :

- a. Cable Theft
- b. Battery Theft
- c. Tarpaulin Theft
- d. Product Theft
- e. Sleeper Theft
- f. Vehicle Theft
- g. Computer Theft
- h. General Theft
- i. Other Specify _____

11. Estimated time of Occurrence : _____

12. Estimated cost : _____

13. Location of Security Occurrence : _____

14. Was the case reported to the Insurer (Yes / No) : _____

- a. If Yes, Name of Insurer : _____
- b. Date Reported : _____

c. Reported By Who : _____

d. Claim No. : _____

15. Was the case reported to the SAPS (Yes/No) : _____

a. Name of Police Station : _____

b. Case No. : _____

c. Name of contact person : _____

d. Contact details : _____

16. Any arrest made (Yes/No) : _____

a. If Yes, how many were arrested : _____

17. Was there a forced Entry? : _____

a. If so, how : _____

Form completed by : _____

Designation : _____

Signature : _____

Date : _____

NOTE:

THIS TECHNICAL FORM DOES NOT REPLACE AN INVESTIGATION OR ANY OF THE LEGISLATIVE FORMS.

Annexure F – Risk rating of penalties

The following penalties shall apply to the Sites for non-compliance of the Service provider in terms of this Agreement:

Penalty Description	Risk rating	Penalty amount	Frequency
Possession & Use of private cell phone by a security officer whilst on duty	High	R500	Per incident
The security officer is on duty without a pocketbook and pen	Low	R50	Per incident
Pocket book of a security officer written up in advance	Low	R50	Per incident
Pocket book not written up hourly	Low	R20	Per incident
The security officer is on duty without an identity disc and/or not wearing required security uniform	High	R530	Per incident
The security officer is on duty without any instrument to determine time or such instrument is not in working condition	Low	R50	Per incident
The security officer is on duty without a flashlight in working order	High	R300	Per incident
The security officer is on duty without a spotlight in working order, where patrol vehicles are not equipped with a spotlight	High	R500	Per incident
There is no operational base radio on Site where required	High	R500	Per shift
The security officer is without a hand-held radio for communication and/or it is not in working order/panic button not working	High	R500	Per incident
A vehicle is without radio communication, or the radio communication is not in working order	High	R500	Per incident
Possession of private firearm by security officer whilst on duty	High	R1000	Per incident
Vehicle not as specified / un-roadworthy / inoperable / unavailable/does not meet safety regulations	High	R500	Per incident
Self-posting and/or no parade or inspection of a security officer	High	R500	Per incident
Late posting of a security officer	High	R500	Per incident
Late submission or non-submission of Health & Safety minutes	High	R100	Per month
No visit from off-Site Supervising Inspector to Site	High	R200	Per incident
Non-attendance of weekly meeting by the Service Provider	High	R500	Per incident
Non-attendance of monthly meetings by managing member, director or designated regional representatives of the Service Provider	High	R500	Per incident
Unavailability of, and non-submission or late submission of any relevant documentation, sheets or failure to complete or keep all relevant documents up to date	High	R200	Per incident
Failure to hand in or late submission of feedback report on the occurrence of an Incident	High	R200	Per incident
Security officer sleeping on duty	High	R1000	Per incident
Security officer under the influence of alcohol/drugs (Permanent removal from TP)	High	R1000	Per incident

Service Level Agreement for the provision of security services at various sites (hereinafter referred to as "the security services") for Transnet SOC Limited (registration number 1990/000900/30) trading as Transnet Property (hereinafter referred to as "TP") for a period of twelve (12) months

CONFIDENTIAL

Security officer/s absent from duty/no security officer deployed/desertion of post	High	R1000	Per incident
Security Officer/Supervisor failed to report an incident	High	R1000	Per incident
Security Officer/Supervisor found in contravention of traffic regulations (i.e. speeding, not wearing seatbelt etc.) in the TP	High	R1000	Per Incident
Negligence by Security Officer/Supervisor in the performance of their duties	High	R1000	Per Incident
Patrol clocking/guard monitoring device not working	High	R500	Per Incident
In the event of the following security officers not being posted or posted late or being absent from his/her place of duty after being posted or under the influence of alcohol or drugs or found sleeping on duty the following penalties shall apply which shall be deducted by the Client from the fees payable to the Service provider, as set out in the Work Document: a) Shift Supervisor b) Site Manager	High	R1000	Per Incident

Annexure G: Removal of Security Officer from Site

TERMINAL	SECURITY OFFICER REMOVAL FORM		Reference Number:	
DETAILS OF OFFICER				
COMPANY NO	NAME OF OFFICER		PSIRA NO	
<p><u>Short description of circumstances leading to the removal of officer from site:</u></p>				
	NAME	SIGNATURE	DATE	DESIGNATION
Requested By				TP Shift Supervisor
Supported By				TP Security Manager
Acknowledged				Security Service Provider