TRANSNET

ACCESS CONTROL STANDARDS FOR SECURITY OFFICIALS OPERATING AT ACCESS AND EGRESS CONTROL POINTS

Policy Reference Number	TCC/SI(01)
Version Number	01
Effective Date	1 July 2022
Review Date	29 June 2022
Policy Owner	Group Security Integration
Signature	
Policy Sponsor	Group Chief of Security
Signature	A. GOVIND
Date Approved	04/07/2022

TABLE OF CONTENTS

1. INTENDED AUDIENCE

Role	Name
Project sponsor	Ashwyn Govind
Business Owner	Cebbie Wolf
Project Manager	Pandelani Swalivha
OD/SBU CSO's	Marius Bennett - (TFR) Hugo Howard - (TP) Neil Naidoo - (TE) Sicelo Tiyo - (TNPA) Richard Sewraj - (TPL) Nico du Plessis - (TPT)
Group Physical Security Functional Heads	Jabulani Moleya, Shawn Johnson
ICT Security, Governance, Risk and Compliance	Daniel Ehrke
GICT Enterprise Technology & PMO	Boitumelo Sathekge

2. BACKGROUND

Access control is legislated by **"The Control of Access to Public Premises and Vehicles Act 53 of 1985"** (CAPPVA) which provides for the safeguarding of certain public premises and vehicles and the protection of people in or at public premises and vehicles. Access/egress control remains important in that it assists with the controlling of movement of people or vehicles into or out of a specific area. Through authentication and authorisation, access control policies make certain users have appropriate access and permission to company premises. Access control can be applied to limit physical access to buildings, offices, and datacentres. The main reason of instituting access control is to ensure effective, seamless, and managed access control movement.

In addition, access control data may be used for purposes of verification, identification and other activities that may aid in other activities such as, investigations.

3. PURPOSE

In order to satisfy a controlled environment, access control points and systems should always be monitored. Constant monitoring of access control points and systems enables the organisation to identify irregularities and implement mitigation plans. As such, it is therefore imperative to institute effective physical access control measures.

4. DEFINITIONS

- **Access Control-** a data security process that enables organisations to manage who is authorised to access premises, corporate data and other resources.
- **Access Point-** a specific point of an access control system.
- **After Hours -**refers to working hours as stipulated in Section 9 of the BEAC, this takes into consideration workplaces that make use of shift hours and operate on a 24-hour basis
- **Authorised People**-refers to people authorised to access certain areas
- **Authorised Vehicle**- refers to vehicles authorised to access certain areas
- **Contractor**- a person or firm that undertakes to provide materials or labour to perform a service or do a job.
- **Employee-**a person employed for wages or salary, especially at non-executive level.
- **POPIA**- refers to the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) to promote the protection of personal information processed by public and private bodies.
- **Protecting Authority-** Refers to Law enforcement agencies such as SAPS, Defence Force, Immigrations Officers, Customs etc.
- **Security Breaches**- Any security incident that results in unauthorised access to premises, applications, services, networks or devices.
- **Unauthorised Vehicle**-Refers to vehicles not authorised to access certain areas

- **Unauthorized People/Persons**- Refers to people/persons not authorised to access certain areas

- **Visitor-**a person visiting someone or somewhere, socially, business or as a tourist.

5. ABBREVIATIONS

- **ISPS-** International Ship and Port facility Security Code
- **ID Book-** Identity Book
- **OHS-** Occupational Health and Safety
- **PFSO-**Port Facility Security Officer
- **POPIA-** Protection of Personal Information Act
- **CSO-**Chief Security Officer
- **SSP-**Ship Security Plan
- **PSIRA-**Private Security Industry Regulation Act
- **SSA-** Ship Security Assessment

6. MINIMUM PROCEDURES TO BE FOLLOWED BY SECURITY OFFICIALS:

6.1. ENTRANCES AND EXIT GATES

6.1.1. Ensure that all entrance and exit gates or booms are always closed.

6.1.2. After hours, all entrance and exit gates must always locked.

6.1.3. Keys of the gates must always be in possession of the guards on duty. Preferable not at the entrance, but at a central control room.

6.1.4. No Security Official is to move in front of a moving vehicle or approach any vehicle from the front. Safe distance must always be 1.5m away from the side of the vehicle.

6.1.5. Ensure that all emergency vehicles coming in and out are given special and urgent attention to avoid delays. Where applicable, emergency vehicles need to be escorted by security personnel to the designated area of emergency.

6.2. PROCEDURE TO BE FOLLOWED DURING ACCESS CONTROL: ARRIVALS AT THE MAIN GATE/ RECEPTION

6.2.1. PEDESTRIANS - EMPLOYEES, CONTRACTOR OR VISITORS

6.2.2. Receive and greet the persons that arrives at Transnet premises access control point, entrances, gates, and receptions.

6.2.3. Establish the purpose of visit.

6.2.4. Request persons to identify themselves and produce proof by means of - Access Card, Identity Document (ID Card/Book), Drivers Licence or Passport. Positive identification must be verified by means of positive and valid identification.

- ***Employees*** - by means of Access Cards. If not in possession of Access Card, the employee must complete the Visitors register and a visitor's access card may be issued.
- ***Visitors and contractors -*** must give their details and purpose of visit. Visitors and contractors should produce positive identification by means of ID book, valid Driver's license or Passport.
  - The person hosting the visitor must be notified by security and ensure that, the visitor is collected at the reception area.
  - The visitor or contractor will be issued with a visitor or contractors' card, which ever one is applicable.

6.2.5. Request persons to declare any items in his/her possession e.g., Laptops, Cell phones, Cameras and/or Firearms. In the case of valuables and firearms, the access control security official must follow the necessary procedures, which include:

- On entering the premises or as a request from a visitor, the item must be declared to the access control Security Officer.

- The access control Security Official completes a register, which lists all the items, gives a description of them and the number of items. It is critical that the access control Security Official makes note of all the details of the item/s.
- A receipt must be issued for all items to be signed by both parties. The items will be placed in a bag or contained and locked in a safe provided for this purpose.
- Items will be reclaimed upon leaving the Transnet premises on presentation of the receipt.
- Carrying of personal firearm is not allowed at Transnet premises unless authorised to do so by a Security Manager.

6.2.6. Search, all persons entering Transnet premises will be expected to be searched.

- ***Employees*** – must be searched, including any baggage or laptop bag and the vehicle boot. Person can be searched by means of handheld metal detectors, walk through scanner, items can be searched manually or by means of X-ray machines.
- ***Visitors and contractors-*** the visitor must be checked with the person being visited. The same methods as indicated above will apply.
- ***Pedestrians-*** pedestrians must be searched using the method indicated above.

6.2.7. Breathalyzer Testing (Where applicable)

- ***All -*** breathalyser testing is to be conducted at the main gate on employees, contractor, sub-contractor, and visitors. "Blow red" or "Positive" incidences of breathalysers results, need to be reported to the Security Manager and OHS Rep immediately and handled according to procedures and policies of Transnet. A person must not be granted access to Transnet premises at all until the procedures has been conducted and the final result of the breathalyser indicates negative. In the event the breathalyser is positive, person may not be granted access to the Trannset premises.

6.2.8. PPE (Where applicable)

- Ensure that all employees are in possession of their correct PPE. Employees, Visitors and Contractor, who are not in possession of correct/appropriate PPE should be referred to the OHS Rep to be assisted/issued, visitors and contractors may also be denied access if they are not properly equipped with PPE. Security to notify OHS Rep immediately.

6.2.9. Granting Access

- ***Employees*** not in possession of Access Card must complete the Visitors register and a visitor's access card must be issued. Thereafter the person can be granted access to his/her workplace.
- ***Visitors and contractors –*** to complete the Visitors register and the information validated by means of ID, Driver's licence or Passport or the person that is visited validating and taking responsibility for the person. A visitor's card must be issued to the person and visitor must return card upon departure. Once the visit is over, the visitor must be escorted back to the egress point by the person that was visited.

6.3. VEHICLES - EMPLOYEES, CONTRACTOR OR VISITORS

6.3.1. Indicate to the driver where to stop, request driver to roll down his/her window. Receive and greet the driver that arrives at Transnet premises access control point, entrances or gate. Employees must move to the designated lane for employees to enter and visitors must be directed to the visitor's lane.

6.3.2. Establish the purpose or reason for visit.

6.3.3. Request driver to identify himself/herself and show proof by means of Access Card, ID, Passport, Permit, Driver's licence or Passport. Positive identification must be presented by means of Access Cards, IDs, Drivers Licenses, Passport and Permit. Driver and passengers must be positively identified.

- ***Employees*** - by means of Access Cards. If not in possession of Access Card, then the person must complete the Visitors register and a visitor's access card must be issued.
- ***Visitors and contractors*** - must give their details and purpose of visit to the access control Security Official. This information should be checked against positive identification e.g., ID book, Valid Driver's license, Passport Permit. The person hosting must be notified by security and ensures that person who is going to be visited collects the visitors at the gate or at reception area.

6.3.4. Request drivers to declare any items- Laptops, Cell phones, Cameras and/or Firearms. In the case of valuables and firearms, the access control Security Official must follow the necessary procedures,

- Upon entering the premises or as a request from a visitor, the item must be declared to the access control Security Officer.

- The access control Security Official completes a register, which lists all the items, gives a description of them and the number of items.
- A receipt will be issued for all items to be signed by both parties. The items will be placed in a bag or contained and locked in a safe provided for this purpose.

- Items will be reclaimed upon leaving the Transnet premises and on presentation of the receipt.

- Drivers and visitors of vehicles who do not have identification, must be requested to move to another side of entrance or to a dedicated waiting area in order not to delay flow of traffic.

6.3.5. Search, all vehicles entering Transnet premises will be expected to be searched.

- All vehicles entering/exiting must be searched.
- Security Officials must inform the driver that their vehicle is liable to be searched before entering Transnet premises.
- Security must request the driver to accompany him/her during the search.
- Security official to request the vehicle be switch off.
- At all times must the driver remains with the guard while the search is conducted.
- Driver must open doors and boot of vehicle and any receptacles in vehicle like briefcases, laptop bags and toolboxes etc.
- If the driver objects to having his vehicle searched, the driver will not be granted access to the Transnet premises.
- If concealed items or stolen items are found when exiting, it must be handled according to the reporting of incidents. All relevant information must be registered in the occurrence book or whatever system the OD is using for security incidents reports.

4.3.6 ***All -*** breathalysers testing is to be conducted at the main gate on employees, contractor, sub-contractor, and visitors in a vehicle. Findings of breathalysers results, need to be reported to the security manager and OHS Rep immediately and handled according to procedures and policies of Transnet. A person must not be granted access to Transnet premises at all until the procedures has been conducted and the final result of the breathalyser indicates negative. In the event the breathalyser is positive, person may not be granted access to the Trannset premises.

6.3.6. PPE and Port Regulations (where applicable)

- All passengers in a vehicle must are in possession of their PPE.
- Delivery or Pick-Up vehicle must switch on their head lights and hazards when moving in harbours.
- Sedan and Bakkies to switch on their lights, hazards and amber roof lights.

6.3.7. Granting Access

- All driver, vehicle details and container information must be registered in the vehicle register before any vehicle enters Transnet premises.
- ***Employees*** in a vehicle who are not in possession of Access Card must complete the Visitors register and a visitor's access card must be issued. Thereafter the person can be granted access to his/her workplace.

- ***Visitors and contractors –*** to complete the Visitors register and the information validated by means of ID, Driver's licence or Passport or the person that is visited validating and taking responsibility for the person.
- A visitor's card must then be issued to the person and then he or she can leave with the person visited. Once the visit is over, the visitor must be escorted back to the egress point by the person that were visited.

7. PROCEDURE TO BE FOLLOWED DURING ACCESS CONTROL: DEPARTURE/ EXITING

7.1. PEDESTRIANS - EMPLOYEES, CONTRACTOR, CONSULTANTS OR VISITORS

7.1.1. Receive and greet persons that are leaving/exiting Transnet premises.

7.1.2. Request the persons to identify themselves and show proof by my means of Access Card, ID, Drivers Licence or Passport. Positive identification must be provided.

- ***Visitors and contractors*** must handback there visitors card and the Visitors Register must be completed when exiting.

7.1.3. Request person to declare any items on his/her e.g., Laptops, Cell phones, Cameras and/or Firearms. In the case of valuables and firearms, the access control security official must follow the necessary procedures, Items that were handed in for safe keeping must be reclaimed upon leaving the Transnet premises on presentation of the receipt. Check Removal Permits, Tool Lists, Standard Tool lists.

7.1.4. Searching, as described, must be adhered to.

Employees – must be searched including any baggage or laptop bag. Persons can be search by means of handheld metal detectors, walk through scanner, items can be searched manually or by means of X-ray machines, walk through scanners or handheld metal detectors.

Visitors and contractors, the visitors or contractor must be checked with the person being visited. The same procedure will be followed as for searching purposes as above.

7.1.5. Granting Exit, wish the person a safe journey and thank them for their cooperation.

7.2. VEHICLES - EMPLOYEES, CONTRACTOR OR VISITORS

7.2.1. Indicate to the driver where to stop, request driver to roll down his/her window. Receive and greet the driver at exit control point or gate. Employees must move to the designated lane for employees to exit and visitors to the visitor's lane.

7.2.2. Request the driver to identify himself/herself and show proof by my means of Access Card, ID, Passport, Permit or Drivers licence or Passport. Driver and passengers must be positively identified.

- **Employees** by means of Access Cards. In the event employees do not have their Access Cards, they will be issued with a visitor's card, and complete the Visitors register.

- ***Visitors and contractors*** must give their name and what was their purpose of visit to the access control security official. This information should be checked against what was registered upon entering the premises.

7.2.3. Request drivers to declare any items on his/her e.g., Laptops, cell phones, cameras and/or firearms in the case of valuables and firearms, the access control security official must follow the necessary procedures, e.g.

- Items will be reclaimed on leaving the Transnet premises on presentation of the receipt

- Drivers of vehicles that has visited or delivered goods to Transnet must have a signed delivery notes or pick-up note/ permit that has been signed off or authorised driver to remove container from harbour or port. Different processes may apply in different terminals, the Terminal System in use will apply.

7.2.4. **Search**

- All vehicles exiting must be searched.
- Security Officials must inform the driver that their vehicle is liable to be searched before exiting Transnet premises.
- Security must request the driver to accompany him/her during the search.
- Security official to request the vehicle be switch off.
- At all times must the driver remain with the guard while the search is conducted.
- Driver must open doors, bonnet, boot of vehicle and any holders in vehicle like briefcases, laptop bags and toolboxes etc.
- If the driver objects to having his vehicle searched, he will not be allowed to exit Transnet premises.

- If concealed items or stolen items are found when exiting, it must be handled according to the reporting of incidents. All relevant information must be registered in the occurrence book or whatever, digital platform adopted.

7.2.5. Granting Exit

- All driver, vehicle details and container information must be registered in the vehicle register before any vehicle exits Transnet premises.

8. ACCESS TO SHIP IN LINE WITH THE ISPS CODE

8.1 The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include any:

- Access ladders
- Access gangways
- Access ramps
- Access doors, side scuttles, windows, and ports
- Mooring lines and anchor chains
- Cranes and hoisting gear

8.2 For each of these, the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level, the SSP should establish the type of restriction or prohibition to be applied and the means to enforce them.

8.3 The SSP should establish for each security level the means of identification required to allow access to the ship and for the individuals to remain on the ship without a challenge. This may involve developing an appropriate identification system, allowing for permanent and temporary identifications for ship's personnel and for visitors respectively. Any ship identification system should, when it is practicable to do so, be co-ordinated with that applying to the port facility. Passengers should be able to prove their identity by boarding passes, tickets etc., but should not be permitted access to restricted areas unless supervised. The SSP should establish provisions to ensure that the identification systems are regularly updated, and that the abuse of procedures should be subject disciplinary action.

8.4 Those unwilling or unable to establish their identity and /or to confirm the purpose of their visit when requested to do so should be denied access to the ship and their attempt to obtain access should be reported, as appropriate, to the SSO, CSO, PFSO and to the national or local authorities with security responsibilities.

8.5 The SSP should establish the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis. The SSP should establish the security measures to control access to the ship in terms of the security levels.

8.6 The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to the control access to them and those to be taken to control activities within them.

8.7 The SSP should ensure that there are clearly established policies to control access to all restricted areas.

8.8 The SSP should provide that all restricted areas should be clearly marked, indicating that access to the area is restricted and that unauthorised presence within the area constitutes a breach of security. Security measures should be applied as per the security level.

9. PERMITS AND WAYBILLS

Security Officers performing access and egress control functions need to take note of the information that needs to be on a waybill. A completed waybill must include the following information:

- **Waybill Number:** An assigned freight bill number.
- **Shipper Number:** If you are the originator of the shipment and responsible for the payment of the invoice, enter your account number here.
- **Consignee Reference Number:** If the consignee is responsible for the shipping charges, enter the consignee's account number.
- **Shipper Information (Form):** Enter your company's name, complete address, telephone number and the name of a shipping contact. Please complete this section completely and accurately. The Shipper's Reference Number is an optional field where a cross-reference number can be entered for your company's internal use.
- **Consignee Information (To):** Enter the consignee's name, complete address, telephone number and contact name. To ensure prompt delivery, please make sure that a contact name is included, that the address is not a Post Office Box and that all in- formation is complete and accurate. The Consignee PO Number is an optional field where an authorization number can be entered as a reference number.
- **Third Party Information:** If neither the shipper nor the consignee is paying the charges, then enter the name, complete address, telephone number,

contact name and account number of the party responsible for payment. The Third Party's account number must be entered in the Third-Party Number box.

- **Declared Value:** If the shipper wants to declare the value of a shipment at an amount higher than Estes Air's limitation of liability, they must do so in this box.
- **Description:** Enter a complete description of the contents of the shipment. If a shipment is palletized, include the number of pieces loaded on each shipping pallet.
- **Dimensions**: Enter the number of pallets and/or pieces in the shipment with the same dimensions on each line. Each piece or pallet with different dimensions (length, width, height and weight) will need to be listed separately.
- **Special Instructions:** Please enter any special instructions relating to the rating or handling of the shipment in this space.
- **Service Requested:** The shipper must check one of the five service levels shown in this section. If no service level is selected, the shipment will default to Next Business Day P.M. service and will be rated accordingly.
- **Shipper's Signature**: It is required that an authorized employee of the shipper sign and print their name in the space provided. By signing the Air Waybill, the shipper verifies that the information on the Air Waybill is complete and accurate. The shipper also acknowledges that Estes Air's terms, conditions and liability apply.
- **Driver Information:** The driver who picks up the freight is required to sign their name and record the date and time of the pickup.

10. REMOVAL PERMITS AND THE REMOVAL OF GOODS/ASSETS

10.1 An approved removal permit must accompany all equipment that leaves Transnet premises, without a permit or standard tool list, no exit will be allowed at Transnet premises.

10.2 Security officials must check the removal permit for authorised signature.

10.3 Security officials must check the material, equipment or item against the amount and item description and that it is according to the removal permit.

10.4 A copy of the removal permit and the persons ID is to be filed and followed up if there is a return-date.

11. DEALING WITH UNAUTHORIZED/AUTHORIZED PEOPLE AND VEHICLES

11.1. To control unauthorized and authorized people, vehicles and goods at an access control point, the following guidelines will make it difficult for unwanted persons to gain access to premises:

Visitors

11.1.1. Have a special visitors parking and issue them with a temporary parking permit (to be returned upon exiting).

11.1.2. Identify entrances and exits for use by visitors. These entrances should be security controlled.

11.1.3. Keep a visitor's register with the following minimum visitors' particulars:

- Name and surname,
- Firm or company represented,
- Reason for visit,
- Time in and out,
- Confirmation of appointment (the person visited),
- Permit/Visitor/Contractor (number) issued before entering and collected before departure.
- All visitors must be escorted when entering a restricted area. Make use of a Security Official or escorted by the host.

Vehicles

11.1.4. A permit system should be in place for authorised vehicles.

11.1.5. The vehicles should be checked prior to entry and before leaving Transnet premises.

11.1.6. Delivery vehicles should be provided for by means of a special permit or detachable sticker and should be checked on arrival and before departing.

12. PROTECTING AUTHORITIES:

All identified South African Police Service (SAPS) and South African National Defence Force (SANDF) personnel have authority to enter a security-controlled site without being searched.

13. PROCEDURES FOR EMERGENCIES AT AN ACCESS AND EGRESS CONTROL POINT

13.1 Identify type/nature of emergency.

13.2 Determine seriousness of emergency.

13.3 Determine immediate threat.

13.4 Respond to the emergency according to the site Emergency Preparedness Plan of the specific site or depot.

13.5 Stabilize the situation, if possible.

13.6 Report immediately to Manager/Supervisor, and Site Manager/Supervisor.

13.7 Make an entry in the Occurrence Book