

## MEMORANDUM

www.transnet.net

---

**To:** Mr. Richard Vallihu, Chief Executive: Transnet National Ports Authority

**From:** Maj. General (Ret.) Rodney Toka: General Manager, Security and Compliance:  
Transnet National Ports Authority

**Date:** 24 October 2016

### **APPROVAL OF THE TRANSNET NATIONAL PORTS AUTHORITY (TNPA) REVIEWED SECURITY POLICY**

---

#### **PURPOSE:**

1. The purpose of this submission is to request approval for the reviewed Transnet National Ports Authority (TNPA), Security Policy. It is a compliance requirement to review the policy annually based on new business requirements and legislations that impact on the Maritime Security environment.

#### **BACKGROUND:**

2. The TNPA Security and Compliance Department is responsible to safeguard (assets, personnel & information), advice, investigate and restore of environment after security incidents for smooth trade facilitation. In carrying-out the mandate, the Head-Office Security office develops and reviews TNPA security policy and procedures.
3. And, based on the above-mentioned security functions, the office has reviewed the Security Policy in consultation with the following key stakeholders:
  - 3.1 Port security Officers (PSOs);
  - 3.2 On the 2 August 2016, consulted with recognised trade unions, UNTU and SATAWU represented by:

- Wiseman Phethwa (UNTU)
  - Regional Goba (SATAWU);
  - Jabulile Madonsela (UNTU), and
  - Ambrose Cele (SATAWU).
- 3.3 Human Resource Management, in particular the Recruitment Office in terms of security screening and Employee Relations Office for inputs.
  - 3.4 Port Performance Review Committee, attendant by port leadership.
  - 3.5 Further consultations were undertaken with TNPA Compliance Office, Ms Rolene Muller to solicit legal inputs.
  - 3.6 Lastly, consulted TNPA Operations Committee (OPCO) on the 16 September 2016, the committee adopted and recommended the policy for presentation and approval by TNPA EXCO meeting.
- 4 All recommendations received from stakeholders were implemented and ready for presentation with possible approval.

#### **DISCUSSION:**

5. The existence of approved policies will serve as a baseline documents to provide clarity in terms of security governance, responsibilities, accountability, direction and reporting of security related matters. Further, guide TNPA security department in implementing and ensuring compliance to security legislative mandates and the ISPS Code. And, most importantly, enhance security measures to:
  - 5.1 Ensure that there is effective co-ordination of security functions at the ports;
  - 5.2 Strengthen the stakeholder management amongst security stakeholders in implementing legislative mandates;
  - 5.3 Secure environment for smooth trade facilitation through the implementation of integrated best practice security model.

#### **FINANCIAL/BUDGET IMPLICATIONS:**

6. There are no financial implications to be suffered in terms of these Policies.

**RECOMMENDATION:**

- 6.1 It is recommended that:
- 6.2 The TNPA Executive Committee approves the renewed security policy to enable the department to enforce the required security legislative mandates.

**COMPILED BY:**



**Solly Mookamedi**

Manager: National Security Operations  
Transnet National Ports Authority

Date: 21/11/2016

**RECOMMENDED BY:**



**Maj. General (Ret.) Rodney Toka**

General Manager: Security and Compliance  
Transnet National Ports Authority

Date: 21/11/2016

**APPROVED BY:**



**Richard Vallihu**

Chairperson: TNPA Executive Committee  
Transnet National Ports Authority

Date:



# **TRANSNET NATIONAL PORTS AUTHORITY**

## **SECURITY POLICY**

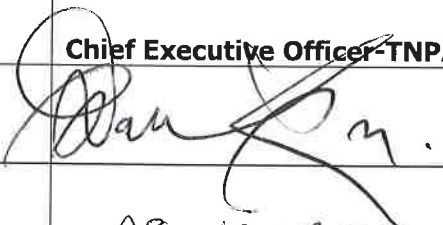
### **DEPARTMENT: PORT**

### **SECURITY**

**and**

### **COMPLIANCE**

## Transnet National Ports Authority: Security Policy

<b>Policy Number:</b>	<b>SMP 1/2015</b>
<b>Version Number:</b>	<b>2</b>
<b>Effective Date:</b>	<b>October 2016</b>
<b>Review Date:</b>	<b>October 2017</b>
<b>Policy Owner</b>	<b>Head of TNPA- Port Security and Compliance Department</b>
<b>Policy Sponsor</b>	<b>Chief Executive Officer-TNPA</b>
<b>Signature</b>	
<b>Date Approved</b>	<b>08.12.2016</b>

## Transnet National Ports Authority: Security Policy

TABLE OF CONTENTS	
1. Statement of Purpose	04
2. Scope	05
3. Legislative Regulatory Requirements	05
4. Policy Statement and Compliance Requirements	06
5. Specific Responsibilities	16
6. Audience	19
7. Enforcement	19
8. Exceptions	20
9. Other Considerations	20
10. Communicating the Policy	20
11. Review and Update Process	21
12. Implementation	21
13. Monitoring of Compliance	21
14. Disciplinary Action	21
15. Approval	22
16 Annexure	23

## Transnet National Ports Authority: Security Policy

### 1. STATEMENT OF PURPOSE

- 1.1 Transnet National Port Authority (TNPA) committed to creating and maintaining a relatively free occupational environment in which our employees, visitors and Service providers will have a peace of mind and where profitability is enhanced by the design, development, implementation, maintenance, evaluating and updating a cost effective Port Security and Compliance Management programme. The success of security programme depends on TNPA personnel, information and other assets to deliver services that ensure the health, safety, security and economic growth and development of our country. TNPA must therefore manage these resources with due diligence and take appropriate measures to protect them against:
  - a. Threats that can cause harm to TNPA, and some economies abroad, that include acts of terror and sabotage, espionage, unauthorised access to buildings and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disasters, technical failures and accidental damage;
  - b. The threat of cyber-attack and malicious activity through the internet is prevalent and can cause severe harm to electronic services and critical infrastructure;
  - c. Threats to the national interests, such as transnational criminal activity, foreign intelligence activities, terrorism and maritime security threats continue to evolve as the result of changes in local, national and international environment.
- 1.2 The Security Policy of TNPA prescribes the application of security measures to reduce the risk of harm that can be caused to the company if the above threats should materialize. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of services. Since TNPA relies extensively on information and communication technology (ICT) to provide its services, this policy emphasizes the need for acceptable use of ICT equipment as well as ICT protection measures to be complied with by employees.
- 1.3 The main objective of this Policy therefore is to support the national interest and TNPA's business objectives by protecting employees, information and other assets and assuring the continued delivery of services to South African citizens and the maritime community.
- 1.4 This Policy complements other TNPA Policies (e.g. sexual harassment, occupational health and safety, official languages, information

## Transnet National Ports Authority: Security Policy

management, asset control, real estate and financial resources).

### 2. SCOPE

**2.1** To create safe and secured working environment, and ensure that the TNPA internal controls are intensified for the effective protection of assets and proprietary Information. This policy applies to the following individuals and entities.

- All TNPA employees;
- All contractors and consultants delivering a service to TNPA, including their employees who may interact with TNPA;
- Temporary TNPA employees
- All information assets of TNPA;
- All intellectual property of TNPA;
- All fixed property that is owned or leased out by TNPA;
- All moveable property that is owned or leased out by TNPA;
- All Facilities operating at TNPA Ports including their employees;
- All private port users
- All State Agencies operating in the Ports
- All Port users with a temporary right of access

**2.2 The Policy further covers the following elements of the security program of TNPA:**

- Security organization
- Security administration
- Information security
- Physical security
- Personnel security
- Information and Communication Technology (ICT) security
- Business Continuity Planning (BCP)

### 3. LEGISLATIVE OR REGULATORY REQUIREMENTS

**3.1** This Policy is informed by and complies with applicable national legislation, international codes, national security policies and national security standards. A list of applicable regulatory documents in this regard has been attached as **Annexure A**.



## Transnet National Ports Authority: Security Policy

### 4. POLICY STATEMENT

**4.1** TNPA will not be sympathetic towards any action of dishonesty, subversion or non-compliance to security measures. Injuries to employees, reputational damage and financial losses that result from crime or misconduct will be viewed in a serious light and be investigated by the Head of Security-Port Security and Compliance Department, consultation with internal and external role players is essential if a relatively crime free working environment is to be created and maintained.

### 4.2 Compliance requirements

**4.2.1** All individuals and institutions mentioned in par. 2 above must comply with the baseline requirements (refer 4.3 below) of this Policy and its associated with Security Directives as contained in the Port Security Plans of TNPA (i.e. security plans of the respective ports). These requirements shall be based on integrated security Threat and Risk Assessments (TRA's) as per the Department of Transport and security cluster standards to the national interest as well as employees, information and assets of TNPA. The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.

### 4.2.2 Security projects and/or programmes execution

All projects and programmes must be prior endorsed by the Head of TNPA Port Security and Compliance, that include amongst others, the following,

- Security Systems Installation;
- Security Audits;
- Surveys;
- Investigations;
- Information requests etc.

### 4.2.3 Staff accountability and acceptable use of assets

**4.2.3.1** The Chief Executive (CE) of TNPA or his delegate shall ensure that information and assets of TNPA are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of TNPA, and other related policies.

**4.2.3.2** All employees of TNPA shall be accountable for the proper utilisation and protection of such information and assets. Employees that misuse, abuse assets, lose, damage assets due to negligent shall be held accountable, therefore disciplinary action shall be taken against any such employee taking into account the Labour Law requirements.

Port Security Plans

See Disciplinary Code

## Transnet National Ports Authority: Security Policy

**4.2.3.3** Compliance with the security policy, procedures and or directives is compulsory

### 4.2.4 Specific baseline requirements

#### 4.2.4.1 Security organization

- a. The CE of TNPA has appointed the Head of Department: Port Security and Compliance to establish and direct a security program and projects to ensure coordination of all policy functions and implementation of this policy requirements;
- b. Given the importance of this role, the Head of Department: Port Security and Compliance with sufficient security experience and training, who is strategically positioned within the organisation to provide the wide strategic advice and guidance to TNPA top management, shall be appointed.
- c. The CE of TNPA must ensure that the Head of Department: Port Security and Compliance has an effective support structure (security component) to fulfil its mandate more effectively, as required by the provisions of the National Ports Act (Act No. 12 of 2005, ISPS Code, relevant legislative mandates, and directives to the satisfaction of internal and external stakeholders referred to in par. 4.3.2 below.
- d. Individuals that will be appointed in the support structure of the Head of Department: Port Security and Compliance must be security professionals with sufficient security education, experience, and training to effectively cope with their respective job functions.

See organizational diagram of the security component.

#### 4.2.5 Security administration

The functions referred to in par. 4.3.1 above are, but not limited to:

- a. General security administration (company directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);
- b. Setting of access limitations;
- c. Administration of security screening (refer par. 4.3.5 below);
- d. Implementing physical security;
- e. Ensuring the protection of employees;
- f. Ensuring the protection of information;
- g. Ensuring ICT security (CCTV & Security control rooms);
- h. Ensuring security in emergency and increased threat situations;
- i. Facilitating business continuity planning;
- j. Ensuring security in contracting; and
- k. Facilitating security reports, breach reporting and investigations.

See detailed functions in the Security Component SOP's in the Security Plan

## Transnet National Ports Authority: Security Policy

### 4.2.6 Security incident/breaches reporting process

- a. Whenever an employee of TNPA, visitors or contractors becomes aware of an incident that might constitute a security breach or a breach of Transnet Ethics or an unauthorised disclosure of information (whether accidentally or intentionally), he/she shall report that to the Head of Department: Port Security and Compliance of TNPA by utilizing the formal reporting procedure prescribed in the Security Breach Directive of TNPA; who will then report to the CE.
- b. The CE of TNPA shall report to the appropriate authority (as indicated in the Security Breach Directive of TNPA) all cases or suspected cases of security breaches, for investigations;
- c. The Head of Department: Port Security and Compliance of TNPA shall ensure that all employees are informed about the procedure for reporting security breaches.

### 4.2.7 Security incidents/breaches response process

- a. The Security Department shall develop and implement security breach response mechanisms for TNPA in order to address all security breaches/ethical breaches/alleged breaches which are reported;
- b. The Head of Department: Port Security and Compliance shall ensure that the CE of TNPA is advised of such incidents as soon as possible;
- c. It shall be the responsibility of the Port Security and Compliance department to ensure that investigations are carried out. Where necessary investigations can be done in conjunction with, State Security Agency Structures (e.g. SSA or SAPS) to conduct further investigation on reported security breaches and provide feedback with recommendations to TNPA. This clause does not preclude any case reporting responsibilities to the mentioned agencies.
- d. Access privileges to classified information, assets and/or to premises may be suspended by the CE of TNPA until administrative, disciplinary and/or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches;
- e. The result of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the CE of TNPA in determining whether to restore, or limit, the security access privileges of an individual or whether to revoke or alter the security clearance of the individual.

See Security Directive:  
Reporting of Security  
Breaches

See Security Directive:  
Security Breaches  
Response Process

## Transnet National Ports Authority: Security Policy

### 4.2.8 Information Security

#### 4.2.8.1 Categorization of information and information classification system

- a. The Head of Department: Port Security and Compliance must ensure that a comprehensive information classification system is developed and implemented at TNPA. All sensitive information produced or processed by TNPA must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure;
- b. All sensitive information must be categorized into one of the following categories in accordance with the applicable legislation:
  - State Secret;
  - Trade Secret; and
  - Personal Information.
- c. And subsequently classified according to its level of sensitivity by using one of the recognized levels of classification:
  - Confidential;
  - Secret; and
  - Top Secret
- d. Employees of TNPA who generate sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labelling of classified documents;
- e. The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times;
- f. Access to classified information will be determined by the following principles:
  - Intrinsic secrecy approach;
  - Need-to-know;
  - Level of security clearance.

See Security Directive:  
Information  
Classification Process

See Security Directive:  
Protection of  
Information: General  
Requirements

## Transnet National Ports Authority: Security Policy

### 4.2.8.2 Physical Security

- a. Physical security involves the proper layout and design of facilities of TNPA and the use of physical security measures to delay and prevent unauthorized access to assets of TNPA. It includes measures to detect attempted or actual unauthorized access and the activation of an appropriate response.
- b. Physical security measures must be developed, implemented, and maintained in order to ensure that the entire personnel, property, and information are secured. These security measures shall be based on the findings of the Threat and Risk Assessment (TRA) conducted by the Head of Department: Port Security and Compliance, Port Security Officer and or delegated personnel.
- c. TNPA shall ensure that physical security is fully integrated with business processes early in the process of planning, selecting, designing, and modifying of its security systems and facilities. TNPA shall:
  - Select, design and modify its security systems and facilities in order to facilitate the effective control of access thereto;
  - Demarcate restricted access areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto;
  - Include the necessary security specifications in planning, request for proposals and tender documentation;
- d. TNPA will also ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms;
- e. All employees, respective State Agents personnel, employees of facilities at the respective ports, private port users, and port users' visitors are required to comply with access control procedures of TNPA at all times. This includes the producing of Corporate ID Cards/permits upon entering any sites of TNPA including ports, the display thereof whilst on the premises and the escorting of official visitors.
- f. All visitors to TNPA restricted areas must be pre-authorised by the Head of Department for the respective area and security shall be notified of intended notices.
- g. All un-authorised access will be a breach of security and internal disciplinary procedures and/ or criminal procedures shall be instituted.

See Security Directive:  
Physical Security



## Transnet National Ports Authority: Security Policy

### 4.2.8.3 Personnel Security

#### 4.2.8.3.1 Security Screening

- a. All employees, contractors and consultants of TNPA, who require access to classified information and critical assets in order to perform their duties or functions, must be subjected to a security screening investigation conducted by the State Security Agency (SSA) so that they could be granted a security clearance at the appropriate level;
- b. The level of security clearance given to a person will be determined by the content of or access to classified information entailed by the post already occupied or to be occupied in accordance with their respective responsibilities and accountability;
- c. Any company, contractor who is providing a security service which may bring them into contact with Transnet confidential, or any kind of intellectual property, the Head of Security must be requested to arrange screening of that entity and their employees by the SSA or any other law enforcement agency, which may enhance the integrity of the procurement process.
- d. A security clearance provides access to classified information subject to the need-to-know principle;
- e. A declaration of secrecy shall be signed by every individual issued with a security clearance to complement the entire security screening process. This will remain valid even after the individual has terminated his/her service with TNPA;
- f. A security clearance will be valid for a period of ten years in respect of the Confidential Level and five years for Secret and Top Secret. This does not preclude re-screening on a more frequent basis as and when need arises and/or as determined by the CE of TNPA, based on information which impact negatively on an individual's security competence;
- g. Security clearances in respect of all individuals who have terminated their services with TNPA shall be immediately withdrawn.

See Security Directive:  
Protection of  
Information: General  
Requirements

See Security Directive:  
Security Screening

#### 4.2.8.3.2 Polygraph Examination

- a. A polygraph examination shall be utilized to provide support to the security screening process. All employees subjected to a Top Secret security clearance will also be subjected to a polygraph examination. The polygraph shall only be used to determine the reliability of the information gathered during the security screening investigation and

## Transnet National Ports Authority: Security Policy

does not imply any suspicion or risk on the part of the applicant;

- b. In the event of any negative information being obtained with regard to the applicant during the security screening investigation (all levels), the applicant shall be given an opportunity to prove his/her honesty and/or innocence by making use amongst others of the polygraph examination. Refusal by the applicant to undergo the examination does not necessarily signify that a security clearance will not be granted.

### 4.2.8.3.3 Transferability of Security Clearances

- a. A security clearance issued in respect of an official from other government institutions shall not be automatically transferable to TNPA. The responsibility for deciding whether the official should be re-screened rests with the CE of TNPA.

### 4.2.8.3.4 Security Awareness and Training

- a. A security training and awareness program must be developed by the Security Department and implemented to effectively and consistently to ensure that all personnel and service providers of TNPA remain security conscious;
- b. All employees shall be subjected to the security awareness and training programs conducted by Port Security and Compliance Department, PSO's in particular and must certify that the contents of the program are available and have been understood and will be complied with. The program will not only cover training with regard to specific security responsibilities but also sensitise employees, relevant contractors and consultants about the security policy, security measures of TNPA as well as the need to protect sensitive information against disclosure, loss or destruction;
- c. Periodic security awareness presentations, briefings, and workshops will be conducted by the Port Security and Compliance Department and in addition to that, posters and pamphlets will be frequently distributed in order to enhance the training and awareness program. Attendance of the above programs will be compulsory for all employees who shall have been identified and notified to attend;
- d. Regular audits, surveys, and walkthrough inspections shall be conducted by the Head of Security or delegated members to monitor the effectiveness of the security program;

See Security Directive:  
Security Screening

See Security Directive:  
Security Training and  
Awareness

## Transnet National Ports Authority: Security Policy

### 4.2.8.3.5 Information and Communication Technology (ICT) Security

#### 4.2.8.3.5.1 ICT Security

- a. A secure network shall be established for TNPA in order to ensure that information systems are secured against rapidly evolving threats that have the potential to impact on their confidentiality, integrity, availability, intended use and value;
- b. To prevent the compromise of ICT systems, TNPA shall implement baseline security controls and any additional control identified through the security TRA. These controls, and the security roles and responsibilities of all personnel, shall be clearly defined by the Head of Security, documented and communicated to all employees;
- c. To ensure policy compliance, the Chief Information Officer of TNPA shall:
  - Certify that all its systems are secure after procurement, accredit ICT systems prior to operation and comply with minimum security standards and directives;
  - Conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis;
  - Periodically request assistance, review, and audits from the state security cluster in order to get an independent assessment.
- d. Server rooms and other related security zones where ICT equipment is kept shall be secured with adequate physical security as defined in the TNPA standard for server and equipment rooms and strict access control shall be enforced and monitored by the ICT in consultation with Security Department;
- e. Access to the resources on the network of TNPA shall be strictly controlled by ICT Department and where access is needed to CCTV or security networks permission must be obtained from the designated Port Security Officer to prevent unauthorized access. Access to all computing and information systems and peripherals of TNPA shall be restricted unless explicitly authorised;
- f. System hardware, operating and application software, the network and communication systems of TNPA shall be adequately configured and safeguarded against both physical attack and unauthorized network intrusion;

See ICT Security Policy and Security Directive: ICT Security



## Transnet National Ports Authority: Security Policy

- g. All employees shall make use of ICT systems of TNPA in an acceptable manner and for business purposes only. All employees shall comply with the IT Security Directives in this regard at all times;
- h. The selection of passwords, their use, and management as a primary means to control access to systems is to strictly adhere to best practice guidelines as reflected in the ICT Security Directives. In particular, passwords shall not be shared with any other person for any reason;
- i. To ensure the on-going availability of critical services, ICT Department shall develop an ICT continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.

See Security Directive:  
ICT Security

### 4.2.8.3.5.2 Internet Access

- a. The Chief Information Officer (CIO) of TNPA, having the overall responsibility for setting up Internet Access for TNPA, shall ensure that the network of TNPA is safeguarded from malicious external intrusion by developing, as a minimum, a configured firewall. Human Resources management shall ensure that all personnel with Internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet;
- b. The CIO of TNPA shall be responsible for controlling user access to the Internet, as well as ensuring that users are aware of the threats, and are trained in the safeguards, to reduce the risk of Information Security breaches and incidents;
- c. Incoming e-mails must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible computer viruses or other malicious code;

See Security Directive:  
ICT Security

### 4.2.8.3.5.3 Use of Laptop Computers

- a. Usage of laptop computers by employees of TNPA is restricted to business purposes only, and users shall be aware of, and accept the terms and conditions of use, especially the responsibility for the security of the asset, and information held on such devices;
- b. The information stored on a laptop computer of TNPA shall be suitably protected at all times, in line with the protection measures prescribed in the IT Security Directive;
- c. Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop

## Transnet National Ports Authority: Security Policy

computers at all times, in line with the protection measures prescribed in the IT Security Directive.

### 4.2.8.3.5.4 Communication Security

- a. The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of TNPA in all its forms and at all times;
- b. All sensitive electronic communications by employees or contractors of TNPA must be encrypted in accordance with the South African Communication Security Agency (SACSA) standards, standards and the Communication Security Directive of TNPA. Encryption devices shall only be purchased from SACSA or COMSEC and will not be purchased from commercial suppliers;
- c. Access to communication security equipment of TNPA and the handling of information transmitted and/or received by such equipment, shall be restricted to authorised personnel only i.e. personnel with a Top Secret Clearance who successfully completed the SACSA Course.

See Security Directive:  
ICT Security

### 4.2.8.3.6 Technical Surveillance Counter Measures (TSCM)

- a. All offices, meeting, conference and boardroom venues of TNPA where sensitive and classified matters are discussed on a regular basis shall be identified and shall be subjected to proper and effective physical security and access control measures. Periodic electronic Technical Surveillance Counter Measures (sweeping) will be conducted by SSA to ensure that these areas are kept sterile and secure;
- b. The Head of Security of TNPA shall ensure that areas that are utilised for discussions of a sensitive nature as well as offices or rooms that house electronic communications equipment, are physically secured in accordance with the standards laid down by SSA in order to support the sterility of the environment after a TSCM examination, before any request for a TSCM examination is submitted;
- c. No unauthorized electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of TNPA is discussed. Authorisation must be obtained from the Head of TNPA Port Security and Compliance Department.

See Security Directive:  
Secure Discussion  
Areas

## Transnet National Ports Authority: Security Policy

### 4.2.8.3.7 Business Continuity Planning (BCP)

- a. The Head of Department: Port Security and Compliance of TNPA must establish a Business Continuity Plan (BCP) to provide for the continued availability of critical services, information and assets if a threat materializes and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of employees, contractors, consultants, facilities, private port users and visitors;
- b. The BCP shall be periodically tested to ensure that the management and employees of TNPA understand how it is to be executed;
- c. All employees of TNPA shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof;
- d. The Business Continuity Plan shall be kept up to date and re-tested periodically by the Head of Department: Port Security and Compliance.

See BCP

## 5. SPECIFIC RESPONSIBILITIES

### 5.1 Chief Executive

- 5.1.1 The CE of TNPA bears the overall responsibility for implementing and enforcing the security programs and projects of TNPA. In executing this responsibility, the CE shall:
  - a. Establish the post of the Head of Security and appoint a well-trained and competent security official in the post;
  - b. Establish a Security Advisory Committee for the company and ensure the participation of all Senior Management members of all core business functions of TNPA in the activities of the Committee;
  - c. Approve and ensure compliance with this Policy and its associated Security Plans and Directives.

### 5.2 Head of Department: Port Security and Compliance

- 5.2.1 The delegated security responsibility lies with the Head of Department: Port Security and Compliance of TNPA who will be responsible for the implementation of TNPA Security Strategy, and programs within TNPA (planning, controlling, organising, activating). In executing his/her responsibilities, the Head of Department: Port Security and Compliance shall, amongst others;

## Transnet National Ports Authority: Security Policy

- a. Chair the TNPA Security and Compliance Management Committee;
- b. Draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of TNPA in conjunction with the Security Committee;
- c. Ensure that Port Security and Port Facility Security Plans are in place and reviewed annually for all regulated ports falling under the TNPA jurisdiction;
- d. Research, develop and or review the Security Policy and Security Plans at regular intervals;
- e. Conduct a security TRA of TNPA with the assistance of the Security Committee;
- f. Advise management on the security implications of management decisions;
- g. Implement a security risk awareness/training program to empower individuals with security functions within the organisation,
- h. Conduct internal security compliance audits and inspections at TNPA at regular intervals;
- i. Conduct preliminary enquiries on security breaches within TNPA;
- j. Strengthen collaborations with security counterparts at national, regional and international level, and liaise with these institutions on a regular basis.
- k. Design and implement an organisational structure that is aligned to and supports the TNPA Security and Compliance Departmental' s goals,

### 5.3 Security Management Committee

- 5.3.1 The Security Committee referred to in par. 5.1.1 above shall consist of senior managers of TNPA representing all main business units of TNPA.
- 5.3.2 Participation in the activities of the Security Committee by the appointed representatives of business units of TNPA shall be compulsory;
- 5.3.3 The Security Committee of TNPA shall be responsible for, amongst others, assisting the Head of Department: Port Security and Compliance in the execution of all security related responsibilities at TNPA, including completing tasks such as drafting/reviewing of the Security Policy and Plan; conducting of a security TRA; conducting of security audits; drafting of BCP; and assisting with security risk awareness and training.

### 5.4 Port Managers

- 5.4.1 All Port Managers have a delegated responsibility and commensurate authority to support security initiatives at their respective regulated ports and advise the Head of Department: Port Security and Compliance's Office about port structural changes and security needs;

See Disciplinary

## Transnet National Ports Authority: Security Policy

- 5.4.2 Port Managers must ensure that appropriate measures are implemented and steps are taken immediately to rectify any non-compliance issues that may come to their attention. This includes taking disciplinary action against employees if warranted.

### 5.5 Port Security Officer (PSO)

A Port Security Officer shall:

- 5.5.1 Manage, lead, co-ordinate, plan and organize the total TNPA security function within a specified port;
- 5.5.2 Carry out duties as specified in the Maritime Security Regulations 2004 and Code of practice on security in ports of Geneva, 2003.
- 5.5.3 Port security Officers shall ensure duties defined in the Port Security Officer's Workbook (as reviewed) are implemented in their respective ISPS regulated Ports.

### 5.6 Port Facilities (Terminal Operators)

- 5.6.1 All Terminal Operators are required to manage their security in accordance with their approved Port Facility Security Plans.
- 5.6.2 All Terminal Operators are required to act upon the security levels as set by the Director General, National Department of Transport.
- 5.6.3 All Terminal Operators are required to comply with all applicable legislation and International Legal Instruments.

### 5.7 Line Management

- 5.7.1 All managers of TNPA shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of TNPA at all times;
- 5.7.2 Managers must ensure that appropriate measures are implemented and steps are taken immediately to rectify any non-compliance issues that may come to their attention. This includes taking disciplinary action against employees if warranted.
- 5.7.3 All Line Managers will ensure that all their staff cooperate with any legitimate security investigation and treat such investigation with the seriousness and confidentiality it deserves.

See Disciplinary

## Transnet National Ports Authority: Security Policy

### 5.8 Port Facility Security Officer (PFSO)

A Port Facility Security Officer shall:

- 5.8.1 Ensure that Port Facility Security Plans are developed in line with the respective overall Port Security Plan;
- 5.8.2 Ensure that regular reviews are held and plans updated accordingly;
- 5.8.3 Carry out functions as per the Maritime Regulations 2004; and the ISPS Code;
- 5.8.4 Report incidents as provided for in Section 62 (5) of the National Ports Authority Act (Act 12 of 2005).
- 5.8.5 Carry out duties as specified in the Maritime Security Regulations 2004 and Code of practice on security, Geneva 2003.

### 5.9 Employees, Consultants, Contractors, and Other Service Providers

- 5.9.1 Every employee, consultant, contractor, various port users and other service provider of TNPA shall know what their security responsibilities are, accept it as part of their normal job function, and not only cooperate, but contribute to improving and maintaining security at TNPA at all times.

## 6 AUDIENCE

- 6.1 This Policy is applicable to all members of the management, employees, consultants, contractors, port facilities & various port users, state security agencies and any other service providers of TNPA. It is further applicable to all visitors and members of the public visiting premises of, or may officially interact with, TNPA.

## 7 ENFORCEMENT

- 7.1 The CE of TNPA and the appointed Head of Security are accountable for the enforcement of this Policy;
- 7.2 All employees of TNPA are required to fully comply with this Policy and its associated Security Directives and Port Facility Security Plans as contained in the Security Plan. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code of TNPA;
- 7.3 Prescripts to ensure compliance to this Policy and the Security Directives by all consultants, contractors, or other service providers of TNPA shall be included in the contracts signed with such individuals/institutions/companies. The consequences of any transgression/deviation or non-compliance shall be clearly stipulated in



## Transnet National Ports Authority: Security Policy

said contracts and shall be strictly enforced. Such consequences may include the payment of prescribed penalties or termination of the contract, depending on the nature of any non-compliance.

### 8 EXCEPTIONS

- 8.1 Deviations from this policy and its associated security directives will only be permitted in cases where material and compelling circumstances merit deviation(s) from particular provision(s) of a policy and procedures, e.g. protection of the people's lives during emergency situations. Written submissions shall be sent to the CE of TNPA, who shall have full authority to grant permission of such request, in whole or in part, or to refuse same, however, each case will be decided based on its merit.

### 9 OTHER CONSIDERATIONS

- 9.1 The following shall be taken into consideration when implementing this Policy:
- 9.1.1 Occupational Health and Safety issues within TNPA operations;
  - 9.1.2 Disaster management at TNPA;
  - 9.1.3 Disabled persons shall not be inconvenienced by physical security measures and must be catered for in such a manner that they have access without compromising security or the integrity of this Policy;
  - 9.1.4 Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).

### 10 COMMUNICATING THE POLICY

- 10.1 The Head of Department: Port Security and Compliance of TNPA shall ensure that the content of this Policy (or applicable aspects thereof) is communicated to all employees, port facilities and various port users, consultants, contractors, other service providers, clients, visitors, members of the public that may officially interact with TNPA. The Head of Department: Port Security and Compliance will further ensure that all security policy and directive prescriptions are enforced and complied with.
- 10.2 The Head of Department: Port Security and Compliance must ensure that a comprehensive security risk awareness program is developed and implemented within TNPA to facilitate the above said communication. Communication of the Policy by means of this program shall be conducted as follows:
- a. Awareness workshops and briefings to be attended by all employees, port facilities and various port users;
  - b. Distribution of memos and circulars to all employees;

## Transnet National Ports Authority: Security Policy

- c. Access to the policy and applicable directives on the intranet of TNPA.

### 11 REVIEW AND UPDATE PROCESS

- 11.1 The Head of Department: Port Security and Compliance, assisted by the Security Committee of TNPA, must ensure that this Policy and its associated Security Directives is reviewed and updated on an annual basis. Amendments shall be made to the Policy and Directives as need arises.

### 12 IMPLEMENTATION

- 12.1 The Head of Department: Port Security and Compliance must manage the implementation process of this Policy and its associated Security Directives (contained in the Security Plan) by means of an action plan (also to be included in the Security Plan of TNPA).
- 12.2 Implementation of the Policy and its associated Security Directives is the responsibility of each and every individual this Policy is applicable to (see par. 2.1 above).

### 13 MONITORING OF COMPLIANCE

- 13.1 The Head of Department: Port Security and Compliance, with the assistance of the security department and Security Committee of TNPA must ensure compliance with this policy and it's associated Security Directives by means of conducting internal security audits and inspections on a frequent basis.
- 13.2 The findings of the said audits and inspections shall be reported to the CE of TNPA forthwith after completion thereof.

See Security Directive:  
Security Audits and  
Inspections

### 14 DISCIPLINARY ACTION


- 14.1 Non-compliance with this Policy and its associated Security Directives shall result in disciplinary action which may include, but is not limited to:
- a. Re-training;
  - b. Verbal and written warnings;
  - c. Termination of contracts in the case of contractors or consultants delivering a service to TNPA;
  - d. Demotions;
  - e. Dismissal;
  - f. Suspension;
  - g. Loss of TNPA information and asset resources access privileges;
- 14.2 Any disciplinary action taken in terms of non-compliance with this Policy



## Transnet National Ports Authority: Security Policy

and its associated directives will be in accordance with the Disciplinary Code of TNPA.

### 15. APPROVAL

**APPROVED BY**  
  
**Mr. R. VALLIHU (CE TNPA)**

**Date:** 12.12.16

### Summary of Changes

No.	Paragraph	Changes
1.	1.1	Modified the statement of purpose
2.	2.1	Modified the security policy scope
3.	4.1	Additions to the policy statement
4.	4.2.2	Modification of threats and risk assessments
5.	4.2.3.3	Additions to staff accountability
6.	4.2.4.1	Modifications to security organisation
7.	4.2.8.2 (b)	Modifications to physical security
8.	4.2.8.3.4(d)	Addition in respect of surveys and inspections
9.	5.2.1	Modifications and additions to Head of TNPA Security responsibilities
10.	5.4.1	Modification to Port Managers responsibilities
11.	8.1	Modification to exception

Version	Status/Changes	Author	Year of Issue
02	Second Issue	Maj. General (Ret.) Rodney Toka (General Manager, Port Security & Compliance)	2016/10

**Distribution:** To all.

## Transnet National Ports Authority: Security Policy

### ANNEXURE 'A' APPLICABLE LEGISLATION AND OTHER REGULATORY FRAMEWORK DOCUMENTS

#### 1. Applicable Legislation

- The Constitution Act 108 of 1996
- 1.2 The National Ports Authority Act 12 of 2005
- 1.3 Control of Access to Public Premises and Vehicles Act 53 of 1985 as amended
- 1.4 The Criminal Procedure Act 51 of 1977 as amended
- 1.5 The Protection of Information Act 84 of 1982 as amended
- 1.6 The Occupational Health and Safety Act 85 of 1993 as amended
- 1.7 The Promotion of Access to Information Act 2 of 2000
- 1.8 Firearms Control Act 60 of 2000
- 1.9 State Information Technology Act 88 of 1998
- 1.10 Private Security Industry Regulation Act 56 of 2001
- 1.11 Trespass Act 6 of 1959 as amended
- 1.12 National Archives of South Africa Act, 43 of 1996
- 1.13 Fire Brigade Services Act, 99 of 1987 as amended
- 1.14 Public Finance Management Act, 1 of 1999
- 1.15 Public Service Regulations, of 2001
- 1.16 The National Strategic Intelligence Act, 39 of 1994
- 1.17 The National Key Points Act 102 of 1980
- 1.18 The Corruption Act, 94 of 1992
- 1.19 Prevention of Organized Crime Act, 121 of 1998
- 1.20 Protected Disclosures Act, 26 of 2000
- 1.21 Telecommunications Act, 2 of 2000
- 1.22 Prevention of Interception and Monitoring Act, 70 of 2002
- 1.23 Electronic Communication Security Act, 68 of 2002
- 1.24 The National Building Regulations and Standards Act, 103 of 1956 as amended
- 1.25 The Prevention and Combating of Corrupt Activities Act 12 of 2004
- 1.26 National Environmental Management Act, 107 of 1995

#### 2. Other Regulatory Framework Documents

- 2.1 Minimum Information Security Standards (MISS), Second Edition March 1998;
- 2.2 Minimum Physical Security Standards (MPSS)
- 2.3 International Ship and Port Facility Security Code and SOLAS Amendments 2002;
- 2.4 Merchant Shipping Act (Maritime Security Regulations) of 2004
- 2.5 Risk Management Standard GRB 1.1 Transnet Generic Security Standard;
- 2.6 White Paper on Intelligence (1995)
- 2.7 SACSA/090/1(4) Communication Security in the RSA
- 2.8 SSA Guidance Documents: ICT Policy and Standards: Part 1 & 2
- 2.9 ISO 17799
- 2.10 National Building Regulations

## Transnet National Ports Authority: Security Policy

### ANNEXURE 'B' GLOSSARY AND DEFINITIONS

- "accreditation" means the official Authorisation by management for the operation of an Information Technology (IT) system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations;
- "assets" means material and immaterial property of an institution. Assets include but are not limited to information in all forms and stored on any media, networks or systems, or material, real property, financial resources, employee trust, public confidence and international reputation;
- "availability" means the condition of being usable on demand to support operations, programmes and services;
- "business continuity planning" includes the development of plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical services and assets;
- "candidate" means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor;
- "certification" means the issuing of a certificate certifying that a comprehensive evaluation of the technical and non-technical security features of an Information and Communication Technology system (hereinafter referred to as an ICT system) and its related safeguards has been undertaken and that it was established that its design and implementation meets a specific set of security requirements;
- "COMSEC" means the organ of state known as the Electronic Communications Security (Pty) Ltd, which was established in terms of section 2 of the Electronic Communications Security Act, 2002 (Act No. 68 of 2002) and until such time as COMSEC becomes operational, the South African Communication Security Agency will be in force;
- "critical service" means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the institution;
- "document" means –
  - any note or writing, whether produced by hand or by printing, typewriting or any other similar process, in either tangible or electronic format;
  - any copy, plan, picture, sketch or photographic or other representation of any place or article;
  - any disc, tape, card, perforated roll or other device in or on which sound or any signal has been recorded for reproduction;
- "information security" includes, but is not limited to ;
  - document security;
  - physical security measures for the protection of information;
  - information and communication technology security;
  - personnel security;
  - business continuity planning;
  - contingency planning;
  - security screening;
  - technical surveillance counter-measures;
  - dealing with information security breaches;
  - security investigations; and

## Transnet National Ports Authority: Security Policy

- administration and organization of the security function at organs of state;
- "National Intelligence Structures" means the National Intelligence Structures as defined in section 1 of the National Strategic Intelligence Act, (Act 39 of 1994);
- "reliability check" means an investigation into the criminal record, credit record and past performance of an individual or private organ of state to determine his, her or its reliability;
- "risk" means the likelihood of a threat materializing by exploitation of a vulnerability;
- "screening investigator" means a staff member of a National Intelligence Structure designated by the head of the relevant National Intelligence Structure to conduct security clearance investigations;
- "security breach" means the negligent or intentional transgression of or failure to comply with security measures;
- "security clearance" means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the need-to-know principle;
- "site access clearance" means clearance required for access to installations critical to the national interests;
- "Technical Surveillance Countermeasures" (TSCM) means the process involved in the detection, localization, identification and neutralization of technical surveillance of an individual, an organ of state, facility, or vehicle;
- "technical/electronic surveillance" means the interception or monitoring of sensitive or proprietary information or activities (also referred to as bugging);
- "threat" means any potential event or act, deliberate or accidental, that could cause injury to persons, compromise the integrity of information or could cause the loss or damage of assets;
- "Threat and Risk Assessment" (TRA) means, within the context of security risk management, the process through which it is determined when to avoid, reduce, and accept risk, as well as how to diminish the potential impact of a threatening event;
- "vulnerability" means a deficiency related to security that could permit a threat to materialize.

## ANNEXURE 'C' SUPPORTING DOCUMENTS

- Security Plan containing the following:
  - Security Component Organization Structure
  - Security Component SOP's
  - Specific Responsibilities of Key Role Players
  - Port Security Plans
  - Security Directive: Reporting of Security Breaches
  - Security Directive: Security Breaches Response Procedures
  - Security Directive: Information Security: General Responsibilities
  - Security Directive: Classification System
  - Security Directive: Minimum Physical Security Standards
  - Security Directive: Security Screening
  - Security Directive: Physical Security
  - Security Directive: Access Control

## **Transnet National Ports Authority: Security Policy**

- Security Directive: ICT Security
- Security Directive: Secure Discussions Areas
- Security Directive: TRA
- Security Directive: Security Audits and Inspections
- ICT Security Policy
- BCP
- OHS Policy
- Disciplinary Code