TRANSNET NATIONAL PORTS AUTHORITY

SECURITY POLICY

PORTFOLIO: LEGAL, RISK & COMPLIANCE

DEPARTMENT: SECURITY

TABLE OF CONTENTS

1. STATEMENT OF PURPOSE

1.1 Transnet National Port Authority (TNPA) depends on its 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.

1.2 Threats that can cause harm to TNPA, and some economies abroad, include acts of terror and sabotage, espionage, unauthorized access to buildings and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disasters, technical failures and accidental damage. The threat of cyber attack and malicious activity through the internet is prevalent and can cause severe harm to electronic services and critical infrastructure. Threats to the national interests, such as transnational criminal activity, foreign intelligence activities and terrorism, continue to evolve as the result of changes in local, national and international environment.

1.3 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.

1.4 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.

1.5 This Policy complements other TNPA Policies (e.g. sexual harassment, occupational health and safety, official languages, information management, asset control, real estate and financial resources).

2. SCOPE

2.1 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 at the Ports
- All Port users with a temporary right of access

2.2 The Policy further covers the following seven 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.

4. POLICY STATEMENT

4.1 General

- Employees of TNPA must be protected against identified threats according to baseline security requirements and continuous security risk management;
- Information and assets of TNPA must be protected according to baseline security requirements and continuous security risk management;
- Continued delivery of services of TNPA must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

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 it's associated Security Directives as contained in the Port Security Plans of TNPA (i.e. Security Plans of the respective Ports). These requirements are/shall be based on integrated security Threat and Risk Assessments (TRA's) 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.	Port Security Plans
4.2.2 Security threat and risk assessments involve: • Establishing the scope of the assessment and identifying the information, employees and assets to be protected; • Determining the threats to information, employees and assets of TNPA and assessing the probability and impact of threat occurrence; • Assessing the security risk based on the adequacy of existing security measures and vulnerabilities; • Implementing any supplementary security measures that will reduce the security risk to an acceptable level.	
4.2.3 Staff accountability and acceptable use of assets	
4.2.3.1 The Chief Executive (CE) of TNPA 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.	
4.2.3.2 All employees of TNPA shall be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse assets of TNPA shall be held accountable therefore disciplinary action shall be taken against any such employee.	See Disciplinary Code
4.3 Specific baseline requirements	
4.3.1 Security organization	
4.3.1.1 The CE of TNPA will/has appointed the Head of Security (National Security Manager) to establish and direct a security program that ensures coordination of all Policy functions and implementation of this Policy requirements;	
4.3.1.2 Given the importance of this role, a Head of Security with sufficient security experience and training who is strategically positioned within TNPA so as to provide institution-wide strategic advice and guidance to senior management, must be appointed.	
4.3.1.3 The CE of TNPA must ensure that the Head of Security has an	See organizational

	effective support structure (security component) to fulfill the functions referred to in par. 4.3.2 below.	diagram of the securit component.
4.3.1.4	Individuals that will be appointed in the support structure of the Head of Security must be security professionals with sufficient security experience and training to effectively cope with their respective job functions.	
4.3.2	**Security administration**	
4.3.2.1	The functions referred to in par. 4.3.1 above are, but not limited to: • General security administration (company directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets); • Setting of access limitations; • Administration of security screening (refer par. 4.3.5 below); • Implementing physical security; • Ensuring the protection of employees; • Ensuring the protection of information; • Ensuring ICT security; • Ensuring security in emergency and increased threat situations; • Facilitating business continuity planning; • Ensuring security in contracting; and • Facilitating security breach reporting and investigations.	See detailed functions the Security Compone SOP's in the Security I
4.3.2.2	**Security incident/breaches reporting process**	
4.3.2.2.1	Whenever an employee of TNPA becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidentally or intentionally), he/she shall report that to the Head of Security of TNPA by utilizing the formal reporting procedure prescribed in the Security Breach Directive of TNPA; who will then report to the CE.	
4.3.2.2.2	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;	
4.3.2.2.3	The Head of Security of TNPA shall ensure that all employees are informed about the procedure for reporting security breaches.	See Security Directive Reporting of Security Breaches
4.3.2.3	**Security incidents/breaches response process**	
4.3.2.3.1	The Security Department shall develop and implement security breach response mechanisms for TNPA in order to address all security breaches/alleged breaches which are reported;	
4.3.2.3.2	The Head of Security shall ensure that the CE of TNPA is advised of such incidents as soon as possible;	

4.3.2.3.3 It shall be the responsibility of the National Intelligence Structures (e.g. NIA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to TNPA;	See Security Directive Security Breaches Response Process
4.3.2.3.4 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;	
4.3.2.3.5 The end 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.	
4.3.3 Information Security	
4.3.3.1.1 Categorization of information and information classification system	
4.3.3.1.1 The Head of Security must ensure that a comprehensive information classification system is developed for 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;	
4.3.3.1.2 All sensitive information must be categorized into one of the following categories: • State Secret; • Trade Secret; and • Personal Information. And subsequently classified according to its level of sensitivity by using one of the recognized levels of classification: • Confidential; • Secret; and • Top Secret	See Security Directive Information Classifica
4.3.3.1.2 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 labeling of classified documents;	
4.3.3.1.3 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;	
4.3.3.1.5 Access to classified information will be determined by the following principles:	See Security Directive Protection of Informat

4.3.5.1.2 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;	
4.3.5.1.3 A security clearance provides access to classified information subject to the need-to-know principle;	
4.3.5.1.4 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;	See Security Directive Security Screening
4.3.5.1.5 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;	
4.3.5.1.6 Security clearances in respect of all individuals who have terminated their services with TNPA shall be immediately withdrawn.	
4.3.5.2 Polygraph Examination	
4.3.5.2.1 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 does not imply any suspicion or risk on the part of the applicant;	
4.3.5.2.2 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.	
4.3.5.3 Transferability of Security Clearances	
4.3.5.3.1 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.	See Security Directive Security Screening
4.3.5.4 Security Awareness and Training	
4.3.5.4.1 A security training and awareness program must be developed	

	by the Security Department and implemented to effectively ensure that all personnel and service providers of TNPA remain security conscious;	
4.3.5.4.2	All employees shall be subjected to the security awareness and training programs and must certify that the contents of the program have been understood and will be complied with. The program will not only cover training with regard to specific security responsibilities but also sensitize 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;	
4.3.5.4.3	Periodic security awareness presentations, briefings and workshops will be conducted 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;	See Security Directive Security Training and Awareness
4.3.5.4.4	Regular audits, surveys and walkthrough inspections shall be conducted by the Head of Security and members of the security department to monitor the effectiveness of the security training and awareness program.	
4.3.6	**Information and Communication Technology (ICT) Security**	
4.3.6.1	**IT Security**	
4.3.6.1.1	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;	
4.3.6.1.2	To prevent the compromise of IT 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, documented and communicated to all employees;	
4.3.6.1.3	To ensure policy compliance, the Chief Information Officer of TNPA shall: • Certify that all its systems are secure after procurement, accredit IT 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 National Intelligence Agency (NIA) in order to get an independent assessment.	See ICT Security Polic and Security Directive ICT Security
4.3.6.1.4	Server rooms and other related security zones where IT equipment is kept shall be secured with adequate physical security measures and strict access control shall be enforced	

	and monitored;	
4.3.6.1.5	Access to the resources on the network of TNPA shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of TNPA shall be restricted unless explicitly authorized;	
4.3.6.1.6	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;	
4.3.6.1.7	All employees shall make use of IT 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;	
4.3.6.1.8	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 IT Security Directives. In particular, passwords shall not be shared with any other person for any reason;	
4.3.6.1.9	To ensure the ongoing availability of critical services, TNPA shall develop IT continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.	See BCP
4.3.6.2	**Internet Access**	
4.3.6.2.1	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;	See Security Directive ICT Security
4.3.6.2.2	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;	
4.3.6.2.3	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;	
4.3.6.3	**Use of Laptop Computers**	
4.3.6.3.1	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 information held on such devices;	
4.3.6.3.2	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;	See Security Directive ICT Security
4.3.6.3.3	Employees shall also be responsible for implementing the appropriate security measures for the physical protection of	

	laptop computers at all times, in line with the protection measures prescribed in the IT Security Directive.	
4.3.6.4	**Communication Security**	
4.3.6.4.1	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;	
4.3.6.4.2	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;	
4.3.6.4.3	Access to communication security equipment of TNPA and the handling of information transmitted and/or received by such equipment, shall be restricted to authorized personnel only i.e. personnel with a Top Secret Clearance who successfully completed the SACSA Course.	See Security Directive ICT Security
4.3.6.5	**Technical Surveillance Counter Measures (TSCM)**	
4.3.6.5.1	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 NIA to ensure that these areas are kept sterile and secure;	
4.3.6.5.2	The Head of Security of TNPA shall ensure that areas that are utilized 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 NIA in order to support the sterility of the environment after a TSCM examination, before any request for a TSCM examination is submitted;	
4.3.6.5.3	No unauthorized electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of TNPA is discussed. Authorization must be obtained from the Head of Security.	See Security Directive Secure Discussion Are
4.3.7	**Business Continuity Planning (BCP)**	
4.3.7.1	The Head of Security 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;	
4.3.7.2	The BCP shall be periodically tested to ensure that the management and employees of TNPA understand how it is to be	

executed;

4.3.7.3 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;

4.3.7.4 The Business Continuity Plan shall be kept up to date and re-tested periodically by the Head of Security.

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 program of TNPA. In executing this responsibility, the CE shall:

- Establish the post of the Head of Security and appoint a well trained and competent security official in the post;
- Establish a **Security Committee** for the company and ensure the participation of all Senior Management members of all the core business functions of TNPA in the activities of the Committee;
- Approve and ensure compliance with this Policy and its associated Security Plans and Directives.

5.2 Head of Security

5.2.1 The delegated security responsibility lies with the Head of Security of TNPA who will be responsible for the execution of the entire security function and program within TNPA (coordination, planning, implementing, controlling,). In executing his/her responsibilities, the Head of Security shall, amongst others;

- Chair the Security Committee of TNPA;
- Draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of TNPA in conjunction with the Security Committee;
- Ensure that Port Security and Port Facility Security Plans are in place and reviewed annually?; for all regulated ports falling under the TNPA jurisdiction
- Review the Security Policy and Security Plan at regular intervals;
- Conduct a security TRA of TNPA with the assistance of the Security Committee;
- Advise management on the security implications of management decisions;
- Implement a security risk awareness program;
- Conduct internal compliance audits and inspections at TNPA at regular intervals;
- Conduct preliminary enquiries on security breaches within TNPA;
- Establish a good working relationship with both NIA and SAPS and liaise with these institutions on a regular basis.

5.3 Security 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 Security 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 manage security at their respective regulated ports and must account on security matters to the Head of Security's Office;

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.

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.

See Disciplinary

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)

5.9 Employees, Consultants, Contractors, and Other Service Providers

5.9.1 Every employee, consultant, contractor, various port users and other service providers 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 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 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 the following circumstances:

- When security can be breached in order to save or protect the lives of people;
- During unavoided emergency circumstances e.g. natural disasters;
- On written permission by the CE of TNPA (reasons for allowing non-compliance to one or more aspects of the Policy and directives shall be clearly stated in such permission; no blanket non-compliance shall be allowed under any circumstances).

See Security Directive Security Training and Awareness

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 Security 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 Security will further ensure that all security policy and directive prescriptions are enforced and complied with.

10.2 The Head of Security 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:

- Awareness workshops and briefings to be attended by all employees, port facilities and various port users;
- Distribution of memos and circulars to all employees;
- Access to the policy and applicable directives on the intranet of TNPA.

See Security Directive Security Audits and Inspections

11 REVIEW AND UPDATE PROCESS

11.1 The Head of Security, 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 Security of TNPA 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 Security, 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.

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:

- Re-training;
- Verbal and written warnings;
- Termination of contracts in the case of contractors or consultants delivering a service to TNPA;
- Dismissal;
- Suspension;
- Loss of TNPA information and asset resources access privileges;

14.2 Any disciplinary action taken in terms of non compliance with this Policy and its associated directives will be in accordance with the Disciplinary Code of TNPA.

15. APPROVAL

APPROVED BY

Mr. K. PHIHLELA (CE TNPA)

Date: 5/11/2008

Summary of Changes:

Version	Status/Changes	Author	Year of Issue
01	Second Issue	MJ Moleya	2008/09

Distribution: To all.

ANNEXURE 'A' APPLICABLE LEGISLATION AND OTHER REGULATORY FRAMEWORK DOCUMENTS

1. Applicable Legislation

1.1 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 NIA Guidance Documents: ICT Policy and Standards: Part 1 & 2
2.9 ISO 17799
2.10 National Building Regulations

ANNEXURE "B" GLOSSARY AND DEFINITIONS

- "accreditation" means the official authorization 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
  - 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: Security Screening
  - Security Directive: Physical Security
  - Security Directive: Access Control
  - 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