dhsps&l
Department:
Human Settlements, Public Safety & Liaison
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

3366 Besemmer STR Telkom building
Industrial site Mafikeng
Private Bag X 2145
Mmabatho
2735

Safety House31-34 Molopo Road
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 381 9101\2\5
Fax: +27 (18) 381 7436

OFFICE OF THE HOD

RECEIVED
07 MAR 2012
SIGN:
DEPARTMENT OF PUBLIC SAFETY

JMkhefa@nwpg.gov.za

DATE : 28 FEBRUARY 2012

TO : ACTING HEAD OF DEPARTMENT

FROM : MANAGEMENT SERVICES AND PLANNING

SUBJECT : SUBMISSION OF SECURITY MANAGEMENT POLICY FOR YOUR SIGNATURE

COMMENTS

Make a copy for Mr Mangoyane
The original to Mr Tinta for safekeeping

HOD`S COMMENT

FILE IN

DEPARTMENT OF PUBLIC SAFETY
NORTH WEST PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA
2012 -02- 28
TEL: 018 381 9104 /117 / 132 FAX: 018 381 9195
PRIVATE BAG X 19, MMABATHO, 2735
HOD RECEIVED CORRESPONDENCE

dhsps&l
Department:
Human Settlements, Public Safety & Liaison
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

3366 Besemmer STR Telkom building
Industrial site Mafikeng
Private Bag X 2145
Mmabatho
2735

Management Services and Planning

Safety House31-34 Molopo Road
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 388 3219
Fax: +27 (18) 381 9123

TO: **ACTING HEAD OF DEPARTMENT**

FROM: **DIRECTOR MANAGEMENT SERVICES AND PLANNING**

DATE: **24 FEBRUARY 2012**

SUBJECT: **SUBMISION OF SECURITY MANAGEMENT POLICY FOR YOUR SIGNATURE**

Background

The draft departmental Security Policy was sent to the Directorate: Legal Services on the 28 September 2011 for legalese and formatting. The response from Legal Services was received on the 26 October 2011 **(Annexure A).** The draft was subsequently distributed to members of the departmental management committee on the 18 November 2011.

Recommendation

It is recommended that the Acting Head of Department attach his signature to the policy in order for it to take effect.

MR. S.M. MATLHAKO
DIRECTOR: MANAGEMENT SERVICES AND PLANNING

dhsps&l
Department:
Human Settlements, Public Safety & Liaison
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

3366 Besemmer STR Telkom building
Industrial site Mafikeng
Private Bag X 2145
Mmabatho
2735

Safety House31-34 Molopo Road
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 388 1380

Our ref 025/LOP/2011

Enq: O.E. Mokgojoa

TO: DIRECTOR – MANAGEMENT SERVICES & PLANNING

FROM: DIRECTOR – LEGAL SERVICES

DATE: 26 OCTOBER 2011

SUBJECT: INPUTS - SECURITY POLICY

The above stated matter bears reference.

Kindly be informed that we have perused the drafted policy document and it was our wish to verify whether it is in line with the Provincial Policy.

Efforts to secure a Provincial Policy from the Head of MISS in the Province however drew a blank and instead we were furnished with a copy belonging to the Premier's Office.

The draft however appears to be in order and is very similar with the one belonging to the Premier's Office.

Hope you will find the above to be in order.

PAUL NAMATE
DIRECTOR – LEGAL SERVICES

DATE.....26/10/11.....

DEPARTMENT OF HUMAN SETTLEMENT, PUBLIC SAFETY AND LIAISON

Public Safety Branch

Security Policy

Revision No: 1 Revision Date: 01/04/2014

DEPARTMENT OF HUMAN SETTLEMENT, PUBLIC SAFETY AND LIAISON
NORTH WEST PROVINCE

Public Safety Branch

VISION

SAFE, SECURED and conducive WORKING ENVIRONMENT

MISSION

ensuring the protection of INFORMATION, assets AND PERSONNEL through implementation of efficient and cost effective security measures

VALUES

CONSCIOUSNESS
INTEGRITY
LOYALTY

TABLE OF CONTENTS		PAGE

POLICY	CROSS REFERENCE
1. POLICY OVERVIEW 1.1 The Department of Public Safety North West Province depends on its personnel, information and assets to deliver services that ensure the safety, security and economic well-being of South African citizens. It must therefore manage these resources with due diligence and take appropriate measures to protect them. 1.2 Threats that can cause harm to Department of Public Safety North West Province, in South Africa and 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 interest, such as transnational criminal activity, foreign intelligence activities and terrorism, continue to evolve as the results of changes in the international environment. 1.3 The Security Policy of Department of Public Safety North West Province prescribes the application of security measures to reduce the risk of harm that can be caused to the institution 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 the Department of Public Safety North West Province 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 the Department of Public Safety North West Province's business objectives by protecting employees, information and assets and assuring the continued delivery of services to South African citizens. 1.5 This policy complements the Department and other Departments, North West Province policies (e.g. sexual harassment, occupational Health and safety, official languages, information management, asset control etc).	

2. SCOPE

2.1 This policy applies to the following:

- ✓ all employees of the Department of Public Safety and Liaison;
- ✓ all contractors and consultants delivering a service to Department, including their employees who may interact with the Department;
- ✓ **temporary employees of the Department;**
- ✓ **all information assets of the Department;**
- ✓ **all intellectual property of the Department;**
- ✓ **all fixed property that is owned or leased by the Department;**
- ✓ **all moveable property that is owned or leased by the Department.**

2.2 The policy further covers the following seven elements of the security program of the Department:

- ✓ **Security organization**
- ✓ **Security administration**
- ✓ **Information security**
- ✓ **Personnel security**
- ✓ **Information and Communication Technology (ICT) security**
- ✓ **Physical security**

3. LEGISLATIVE AND REGULATORY REQUIREMENTS

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

4. POLICY STATEMENT

4.1 General

- ✓ **Employees, information and assets of the Department must be protected against identified threats as well as continued delivery of service including business continuity planning according to baseline security requirements and continuous security threat and risk management.**

4.2 Compliance requirements

4.2.1 All individuals mentioned in par. 2 above must comply with the baseline requirements of this policy and its association Security Directives as contained in the Security Plan of the Department.

4.2.2 Security threat and risk assessment 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 the Department and assessing the probability and impact of threat occurrences;**
- ✓ **Assessing the risk based on the adequacy of existing security measures and vulnerabilities;**
- ✓ **Implementing any supplementary security measures that will reduce the risk to an acceptable level.**

4.2.3 Staff accountability and acceptable use of assets

4.2.3.1 Officials of the Department shall ensure that information and assets of the Department are used in accordance with procedures as stipulated in the Security Directives.

4.2.3.2 All employees of the Department shall be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse assets of the Department shall be held accountable therefore and disciplinary action shall be taken against any such employee.

4.3 Specific baseline requirements

4.3.1 Security organisation

4.3.1.1 The HOD of the Department will appoint a Security Manager (SM) to establish and direct a security program that ensures coordination of all policy functions and implementation of the policy.

4.3.1.2 Given the importance of this role, a Security Manager shall provide institution with security advice and guidance to senior management.

4.3.1.3 The HOD of the Department will ensure that the Security Manager has an effective support structure (security component) to fulfill the functions referred to in par 4.3.2 below.

4.3.1.4 Individuals that will be appointed in the support structure of the

Security Manager will all 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 include:

- ✓ **General security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);**
- ✓ **Setting of access limitations**
- ✓ **Administration of security screening;**
- ✓ **Implementation of physical security;**
- ✓ **Ensuring the protection of employees;**
- ✓ **Ensuring the protection of information;**
- ✓ **Ensuring ICT security;**
- ✓ **Ensuring security in emergency and increased threat situations;**
- ✓ **Ensuring security in contracting; and**
- ✓ **Facilitating security breach reporting and conduct security investigations.**

4.3.2.2 Security incident/breaches reporting process

4.3.2.2.1 Whenever an employee of Department 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 Security Manager of Department by utilizing the formal reporting procedure prescribed in the Security Breach Directives of the Department.

4.3.2.2.2 The Security Manager of the Department shall report to the HOD and appropriate authority (as indicated in the Security Breach Directive of the Department all cases or suspected cases of security breaches, for investigation.

4.3.2.2.3 The Security Manager of the Department shall ensure that all employees are informed about the procedure for reporting security breaches.

4.3.2.3 Security incident/breaches response process

4.3.2.3.1 The Security Manager shall develop and implement security breach response mechanisms for the Department in order to address all security breaches/alleged breaches which are reported.

4.3.2.3.2 The Security Manager shall ensure that the HOD of the Department is advised of such incidents as soon as possible.

4.3.2.3.2 It is the responsibility of the National Intelligence Structures (e.g. NIA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendation to the Department.

4.3.2.3.4 Access privileges to classified information, assets and/or to premises may be suspended by the HOD of the Department until the administrative, disciplinary and/or criminal processes have been concluded, following the investigations into security breaches or alleged security breaches.

4.3.2.3.5 The end results of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the HOD of the Department 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 Categorization of information and information classification system

4.3.3.2 The Security Manager must ensure that a comprehensive information classification system is developed and implemented in the Department. All sensitive information produced or processed by Department must be identified, categorized and classified according to the author, against loss or disclosure.

4.3.3.3 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 recognised levels of classification:

- ✓ Confidential;
- ✓ Secret; and
- ✓ Top Secret

4.3.3.4 Employees of Department 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.

4.3.3.5 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.

4.3.3.6 Access to classified information will be determined by the following principles:

- ✓ Intrinsic secrecy approach;
- ✓ Need-to-know;
- ✓ Level of security clearance

4.3.4 Personnel Security

4.3.4.1 Security Screening

4.3.4.1.1 All employees, contractors and consultants of Department, who requires access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security screening investigation conducted by the National Intelligence Agency (NIA) in order to be granted a security clearance at the appropriate level.

4.3.4.1.2 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.

4.3.4.1.3 A security clearance provides access to classified information subject to the need-to-know principle.

4.3.4.1.4 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 services with the Department.

4.3.4.1.5 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 determined by the HOD, based on information which impact negatively on an individual's security competence.

4.3.4.1.6 Security clearance in respect of all individuals who have terminated their services with Department must be immediately withdrawn.

4.3.4.2 Polygraph examination (National Intelligence Agency)

4.3.4.2.1 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 polygraph examination. The polygraph examination 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.

4.3.4.2.2 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 of the polygraph examination. Refusal by the applicant to undergo the examination does not necessarily signify that a security clearance will not be granted.

4.3.4.3 Transferability of security clearances

4.3.4.3.1 A security clearance issued in respect of an official from other government institutions shall not be automatically transferable in respect of all individuals who have terminated their services with Department. The responsibility for deciding whether the official should be rescreened rests with the HOD of the in respect of all individuals who have terminated their services with Department.

4.3.4.4 Security awareness and Training

4.3.4.4.1 A security and awareness program must be/has been developed by the Security Manager and implemented to effectively ensure that all personnel and service providers of Department remain

security conscious.

4.3.4.4.2 All employees shall be subjected to the security awareness and training programs and must certify that the contents of the program(s) has been understood and will be complied with. The program must cover(s) training with regard to specific security responsibilities and sensitize employees and relevant contractors and consultants about the security policy and security measures of Department and the need to protect sensitive information against disclosure, loss or destruction.

4.3.4.3.3 Periodic security awareness presentations, electronic awareness, briefings and workshops will be conducted as well as posters and pamphlets frequently distributed in order to enhance the training and awareness program. Attendance of the above programs is compulsory for all employees identified and notified to attend the events.

4.3.4.3.4 Regular surveys and walkthrough inspections shall be conducted by the Security Manager (SM) and members of the security component to monitor the effectiveness of the security training and awareness program.

4.3.5 Information and Communication Technology (ICT) Security

4.3.5.1 ICT Security

4.3.5.1.1 A secure network shall be established for Department 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.

4.3.5.1.2 To prevent the compromise of ICT systems, Department shall implement baseline security controls and any additional control identified through the Security Threat and Risk Assessment. These controls, and the security roles and responsibilities of all personnel, shall be clearly defined, documented and communicated to all employees.

4.3.5.1.3 To ensure policy compliance, the IT manager of Department shall:

- ✓ **Certify that all its systems are secure after procurement, accredit ICT systems prior to operation and comply with minimum security standards and deliveries;**

- ✓ 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.

4.3.5.1.4 Server rooms and other related security zones where IT equipment are kept shall be secured with adequate physical security measures and strict access control shall be enforced and monitored.

4.3.5.1.5 Access to the resources on the network of Department shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of the Department shall be restricted unless explicitly authorized.

4.3.5.1.6 Systems hardware, operating and application software, the network and communication systems of Department shall all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

4.3.5.1.7 All employees shall make use of ICT systems of the Department in an acceptable manner and for business purposes only. All employees shall comply with the ICT security Directives in this regard at all times.

4.3.5.1.8 The selection of password, 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.

4.3.5.1.9 To ensure the ongoing availability of critical services, Department shall develop ICT continuity plans as part of its overall Business Continuity Planning (BCP) and IT disaster recovery plan.

4.3.5.2 Internet Access

4.3.5.2.1 The IT manager of Department, having the overall responsibility for setting up Internet access for Department, shall ensure that the network of Department is safeguarded from malicious external intrusion by deploying 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.

4.3.5.2.2 The IT Manager/ systems administrator of Department shall be responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security breaches and incidents.

4.3.5.2.3 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.

4.3.5.3 Use of laptop computers

4.3.5.3.1 Usage of laptop computers by employees of Department 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 Information held on such devices.

4.3.5.3.2 The information stored on a laptop and computer shall be suitably protected at all times, in line with the protection measures prescribed in the ICT Security Directives.

4.3.5.3.3 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 ICT Security directives.

4.3.5.4 Communication security

4.3.5.4.1 The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of Department in all its forms and at all times.

4.3.5.4.2 All sensitive electronic communications by employees, contractors or employees of Department must be encrypted in accordance with the South African Communication Security Agency (SACSA) standards, COMSEC standards and the communication Security Directives of Department. Encryption devices shall only be purchased from SACSA or COMSEC and will not be purchased from commercial suppliers.

4.3.5.4.3 Access to communication security equipment and the handling of information transmitted and/or received by such equipment, shall be restricted to authorized personnel only (personnel with a Top Secret Clearance who successfully completed the SACSA Course).

4.3.5.5 Recording PA System and cell phone network blocker

4.3.5.5.1 All offices, meeting, conference and boardroom venues of Department where sensitive and classified matters that are discussed on a regular basis shall be identified and shall be subjected to proper and effective physical security and access control measures. The Sub – directorate MISS must be invited to implement necessary measures.

4.3.5.5.2 The Security Manager 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.

4.3.5.5.3 No unauthorised electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of Department is discussed. Unauthorization must be obtained from the Security Manager.

4.3.6 Physical Security

4.3.6.1 Physical security involves the proper layout and design of facilities of the Department and the use of physical security measures to delay and prevent unauthorized access to assets of the Department. It includes measures to detect attempted or actual unauthorised access and the activation of an appropriate response. Physical security also includes the provision of measures to protect employees from bodily harm.

4.3.6.2 Physical security measures must be developed, implemented and maintained in order to ensure that the entire Department, its personnel, property and information are secured. These security measures shall be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Manager (SM).

4.3.6.3 The Department shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities. The Department shall:

- ✓ Select, design and modify facilities in order to facilitate the effective control of access thereto;
- ✓ Demarcate restricted access areas (where applicable) 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;
- ✓ Incorporate related costs in funding requirements for the implementation.

4.3.6.4 Department 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.

4.3.6.5 All employees are required to comply with access control procedures of Department at all times. This includes the producing of ID Cards upon entering any site of the Department, the display thereof whilst on the premises and the escorting of official visitors.

5. SPECIFIC RESPONSIBILITIES

5.1 Head of Department

5.1.1 The HOD bears the overall responsibility for implementing and enforcing the security programs, the HOD shall:

- ✓ Establish the post of the Security manager and appoint a well trained and competent security official in the post;
- ✓ Establish a security committee for the institution and ensure the participation of all senior management members of all the core business functions of Department in the activities of the committee;
- ✓ Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

5.2 Security Manager

5.2.1 The delegated security responsibility lies with the Security Manager of the Department who will be responsible for the execution of the entire security function and program within the Department (coordination, planning, implementing, controlling, etc). Towards execution of his/her responsibilities, the Security Manager shall, amongst others,:

- ✓ Chair the security committee of the Department;
- ✓ Draft the internal Security Policy and Security Plan (containing the

specific and detailed Security Directives) of Department of Public Safety North West Province in conjunction with the security committee;

- ✓ Review the Security Policy and Security Plan at regular intervals;
- ✓ Conduct a security TRA of Department of Public Safety North West Province with the assistance of the security committee;
- ✓ Advise management on the security implications of management decisions;
- ✓ Implement a security awareness program;
- ✓ Conduct internal compliance audits and inspections at Department of Public Safety North West Province at regular intervals;
- ✓ 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 Department representing all the main business units of Department.

5.3.2 Participation in the activities of the Security Committee by the appointed representatives of business units of Department shall be compulsory.

5.3.3 The Security Committee of the Department shall be responsible for, amongst others,;

- ✓ Assist the Security Manager in the execution of all security related responsibilities at Department , including completing tasks such as drafting/reviewing of the Security Policy and Plan, conducting of a security TRA, conducting of security audits, drafting of a BCP and assisting with security awareness and training.

5.4 Line Management

5.4.1 All managers of Department shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of Department at all times.

5.4.2 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 the taking of disciplinary action against employees if warrant.

5.5 Employees, Consultants, Contractors and other Service Providers

5.5.1 Every employee, consultant, contractor and other service providers of Department 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 Department at all times.

6. AUDIENCE

6.1 This Policy is applicable to all members of the management, employees, consultants, contractors and any other service providers of Department. It is further applicable to all visitors and members of the public visiting premises of or may officially interact with Department.

7. ENFORCEMENT

7.1 The HOD must appoint a Security Manager who is responsible for the enforcement of the Departmental Security Policy.

7.2 All employees of the Department are required to fully comply with associated Security Directives as contained in the Security Policy. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code/Regulation of Department.

7.3 Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of Department shall be included in the contracts signed with such individuals/institutions/companies. The consequences of any transgression/deviation or non-compliance shall clearly be stipulated in all contracts and shall be 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 Deviation from this policy and its associated Security Directives will only be permitted in the following circumstances:

- ✓ **When security must be breached in order to save or protect the lives of people;**
- ✓ **During unavoidable emergency circumstances e.g. natural disasters;**
- ✓ **On written permission of the HOD (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).**

9. OTHER CONSIDERATIONS

9.1 The following shall be taken into consideration when implementing this policy:

9.1.1 Occupational Health Safety and Safety issues in the Department.

9.1.2 Disasters management at Department.

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).

. COMMUNICATING THE POLICY

10.1 The Security Manager of the Department shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees, consultants, contractors, service providers, clients, visitors, members of the public that may officially interact with Department. The Security Manager will further ensure that all security policy and directive prescriptions are enforced and complied with.

10.2 The Security Manager must ensure that a comprehensive security awareness program is developed and implemented within Department of Public Safety North West Province 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;**
- ✓ **Distribution of memos and circulars to all employees;**
- ✓ **Access to the policy and applicable directives on the intranet of Department of Public Safety North West Province.**

11. REVIEW AND UPDATE PROCESS

11.1 The Security Manager, assisted by the Security Committee of Department of Public Safety North West Province, 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 the need arise.

12. IMPLEMENTATION

12.1 The Security Manager of Department of Public Safety North West Province 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 Department of Public Safety North West Province .

12.2 Implementation of the policy and its associated Security Directives is the responsibility of each and every individual this policy is applicable too (see par 2.1 above).

13. MONITORING COMPLIANCE

13.1 The Security Manager, with the assistance of the security component and security committee of Department of Public Safety North West Province must ensure compliance with this policy and its associated Security Directives by means of conducting internal security audits and inspections on a frequent basis.

13.2 The findings of said audits and inspections shall be reported to the HOD of Department of Public Safety North West Province 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 are not limited to:

- ✓ Re-training;
- ✓ Verbal and written warnings;
- ✓ Termination of contracts in case of contractors or consultants delivering a service to Department of Public Safety North West Province ;
- ✓ Dismissal;
- ✓ Suspension;
- ✓ Loss of Department of Public Safety North West Province 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/directive of the Department.

Approved by Acting Head of Department

.....

Mr. B.T. Mahlakoleng

Date: 05/03/2012

ANNEXURE: A APPLICABLE LEGISLATION AND OTHER REGULATORY FRAMEWORK DOCUMENTS

Applicable legislation

- ✓ Constitution of the Republic of South African, 1996 (Act 106 of 1996)
- ✓ Protection of Information Act, 1982 (Act no 84 of 1982)
- ✓ Promotion Access to Information Act, 2000 (Act no 2 of 2000)
- ✓ Promotion of Administration Justice Act, 2000 (Act no 3 of 2000)
- ✓ Copyright Act, 1978 (Act no 98 of 1978)
- ✓ National Archives of South Africa Act, 1996 (Act no 43 of 1996) and regulations
- ✓ Public Service Act, 1994 (Act no 103 of 1994) and regulations
- ✓ Occupational Public Safety and Safety Act, 1993 (Act no 85 of 1993)
- ✓ Criminal Procedure Act, 1977, (Act 51 of 1977), as amended.
- ✓ Private Security Industry Regulation Act, 2001 (Act 56 of 2001)
- ✓ Control of Access to Public premises and Vehicle Act, 1985 (Act 53 of 1985)
- ✓ National Key Point Act, 1980 (Act 102 of 1980)
- ✓ Trespass Act, 1959 (Act 6 of 1959)
- ✓ Electronic Communication and Transaction Act, 2002 (Act 25 of 2002)
- ✓ Electronic Communication Security (Pty) Ltd Act, 2002 (Act 68 of 2002)
- ✓ State Information Technology Agency Act, 1998 (Act 88 of 1998)
- ✓ Regulation of interception of Communications and provision of Communication-related Information Act, 2002 (Act 70 of 2002)
- ✓ General Intelligence Law Amended Act, 2000 (Act 66 of 2000)
- ✓ Intelligence Service Act, 2002 (Act 65 of 2002) and regulations
- ✓ National Strategic Intelligence Act, 1994 (Act 39 of 1994)
- ✓ Intelligence Service Control Act, 1994 (Act 40 of 1994)
- ✓ Labour Relations Act, 1995 (Act 66 of 1995)
- ✓ Employment Equity Act, 1998 (Act 55 of 1998)
- ✓ Fire –arms Control Act, 2000 (Act 60 of 2000) and regulations
- ✓ Non-proliferation of Weapons of Mass Destruction Act, 1993 (Act 87 of 1993)
- ✓ Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act 33 of 2004)
- ✓ National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
- ✓ Protected Disclosure Act, 2000 (Act 26 of 2000)
- ✓ Intimidation Act, 1982 (Act 72 of 1982)
- ✓ Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 of 2004)
- ✓ Public Finance Management Act, 1999 (Act 1 of 1999) and Treasury Regulations

Other regulatory framework documents

- ✓ Minimum Information Security Standards (MISS), Second Edition March 1998
- ✓ White paper on Intelligence (1995)
- ✓ SACSA/090/1(4) Communication Security in the RSA
- ✓ NIA Guidance Documents: ICT Policy and Standards: Part 1 & 2
- ✓ ISO 17799

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 consideration;
- ✓ "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 as Electronic Communication 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;
- ✓ "CRITICAL SERVICE" means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise and the compromise of which will endanger the effective functioning of the institution;
- ✓ "DOCUMENT" means –
  - ➢ Any note 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 investigation; and
- Administration and organization of the security function at organs of state;

- ✓ "NATIONAL INTELLIGENCE STRUCTURES" means the National Intelligence Structures as defined in section1 of the National Strategic Intelligence 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 investigation;
- ✓ "SECURITY BREACH" means the negligent or intentional transgression of or failure to comply with security measures;
- ✓ "SECURITY CLEARANCE" means a certificate issued to candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subjected to the need to know;
- ✓ "SITE ACCESS CLEARANCE" means clearance required for access installations critical to the national interest;
- ✓ "TECHNICAL SURVEILLANCE COUNTER MEASURES" (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, comprehensive 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 Organizational Structure
  - ➢ Security Component SOP's
  - ➢ Specific Responsibilities of Key Role Players
  - ➢ Security Directive: Reporting of Security Breaches and Response Procedure
  - ➢ Security Directive: Information Security: General Responsibility
  - ➢ Security Directive: Classification System
  - ➢ Security Directive: Security Screening
  - ➢ Security Directive: Physical Security
  - ➢ Security Directive: Access Control
  - ➢ Security Directive: ICT Security
  - ➢ Security Directive: Secure Discussion Areas
  - ➢ Security Directive: TRA
  - ➢ Security Directive: Security Audits and Inspection

- ✓ OHS Policy
- ✓ Disciplinary Code