

the dr&pw

Department:
Roads and Public Works
NORTHERN CAPE PROVINCE
REPUBLIC OF SOUTH AFRICA

DEPARTMENTAL SECURITY POLICY

Version 7 (13March 2013)

TABLE OF CONTENTS

Contents	Page
1. DEFINITIONS.....	4
2. INTRODUCTION.....	7
3. REGULATORY FRAMEWORK.....	7
4. OBJECTIVE.....	8
5. PRINCIPLES, VALUES AND PHILOSOPHY.....	8
6. SCOPE AND APPLICABILITY.....	8
7. PROCEDURES.....	9
7.1 Compliance Requirements.....	9
7.2 Staff accountability and acceptable use of assets.....	9
7.3 Specific baseline requirements.....	9
7.3.1 Security administration.....	9
7.4 Security incidents/breaches reporting process.....	10
7.5 Security incidents/breaches response process.....	10
7.6 Information Security.....	11
7.6.1 Categorization of information and information classification..... system	11
7.7 Physical Security.....	13
7.8 Personnel Security.....	14
7.8.1 Security screening.....	14
7.9 Polygraph Screening.....	15
7.10 Transferability of security clearance.....	15
7.11 Security awareness and training.....	15
7.12 Information and Communication Technology (ICT).....	16
7.12.1 Information Technology (IT) security.....	16
7.13 Internet Access.....	17
7.14 Use of Laptop Computers.....	17
7.15 Communication Security.....	18
7.16 Technical Surveillance Counter Measures (TSCM).....	18
8. BUSINESS CONTINUITY PLAN (BCP).....	19

9.	ROLES AND RESPONSIBILITIES.....	19
9.1	The Head of Department.....	19
9.2	The Security Manager.....	19
9.3	The Security Committee.....	20
9.4	Programme Managers.....	20
9.5	Employees, Contractors, Consultants and other Service Providers.....	20
10.	ENFORCEMENTS.....	20
11.	EXCEPTIONS.....	21
12.	OTHER CONSIDERATIONS.....	21
13.	COMMUNICATING THE POLICY.....	21
14.	FINANCIAL IMPLICATION.....	22
15.	MONITORING AND EVALUATION.....	22
16.	DISCIPLINARY ACTION.....	22
17.	POLICY REVIEW.....	22
18.	APPROVALS AND RECOMMENDATIONS.....	23

1. DEFINITIONS

"Access Control"	The process by which access to a particular area is controlled or restricted to authorised personnel only. This is synonymous with controlled access.
"Accredited"	Means the process of the official authorization by management for the operation of an Information Technology (IT) system; and acceptable by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations. The state information technology agency (SITA) is predominantly responsible for accrediting IT service providers.
"Assets"	Means material and immaterial and intellectual property of an institution. Assets include, but are not limited to information in all forms stored on any media, network or systems or material, real property, financial resources, employee trust, public confidence and international reputation.
"Classification"	The process whereby all official matters exempted from undue disclosure are labelled Confidential, Secret or Top Secret.
"Contingency Planning"	The prior planning of any action that has the Purpose to prevent, and/or combat, or counteract the effect and results of an emergency situation where lives, property or information are threatened.
"Declaration"	An undertaking given by a person who will have, has or has had access to classified / sensitive information, that he / she will treat such information as secret.
"Department (DRPW)"	Department of Roads and Public Works,

	Northern Cape Province.
"Document"	In terms of the Protection of Information Act, Act 84 of 1982, a document is any note or writing, whether produced by hand or by printing, typewriting or any other similar process, any copy, plan, sketch or photographic or other representation of any place or article or any disc, tape, card, perforated roll or other device, in, or on which sound or any signal has been recorded for reproduction.
"Document Security"	Means the application of security measures in order to protect classified / sensitive documents.
"Information Security"	Means the application of a system to implement personnel, physical, computer, and communication security measures to protect sensitive information.
"National Intelligence Structures"	Means the National Intelligence Structures as defined in Section 1 of the National Strategic Intelligence Act, Act 39 of 1994.
"Personnel security"	Personnel security is that condition created by the conscious provision and application of security measures in order to ensure that any person who gains access to sensitive / classified information has the necessary security clearance, and conducts himself / herself in a manner not exposing him / her or the information to compromise. This could include mechanisms to effectively manage / solve personnel grievances and disciplinary matters.
"Physical security"	That condition which is created by the conscious provision and application of physical security measures for the protection of persons, property and information.

"Risk"	Means the likelihood of a threat materializing by exploitation of vulnerability.
"Screening Institution"	Are those institutions, namely the South African Police Service (SAPS), the State Security Agency (SSA), the South African Secret Service (SASS), and the South African National Defence Force (SANDF) that, in terms of the rationalisation agreement, are responsible for the security screening / vetting of persons within their jurisdictions. SSA has a legal mandate to employees within the Public Service.
"Security audit"	Refers to a process conducted to determine if recommendations made in a previous security assessment has been implemented.
"Security breach"	Means the negligent or intentional transgression of or failure to comply with security measures.
"Security clearance"	It is a process whereby an official is given access to official documents in line with the inherent requirements of the job, indicating the degree of security competence of such an official. It is an official document that indicates the degree of security competence of a person.
"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.

2. INTRODUCTION

This policy seeks to protect the employees, information and assets of the Department of Roads and Public Works against identified threats according to baseline security requirements and continuous risk management.

3. REGULATORY FRAMEWORK

This policy is informed by and complies with applicable National Legislation, National Security Policies and National Security Standards. A list of all applicable regulatory documents in this regard are as follows:

- 3.1 Control of Access to Public Premises and Vehicles Act, Act No. 53 of 1985.
- 3.2 Criminal Procedure Act, Act No. 51 of 1977, as amended.
- 3.3 Private Security Industry Regulations Act, Act No. 56 of 2001.
- 3.4 Protection of Information Act, Act No. 84 of 1982.
- 3.5 Promotion of Access to Information Act, Act No. 2 of 2000.
- 3.6 Promotion of Administrative Justice Act, Act No. 3 of 2000.
- 3.7 National Archives of South Africa Act, Act No. 43 of 1996.
- 3.8 Occupational Health and Safety Act, Act No. 85 of 1993, as amended.
- 3.9 Constitution of the Republic of South Africa, Act 108 of 1996.
- 3.10 National Key Points Act, Act No. 102 of 1980.
- 3.11 Trespass Act, Act No.6 of 1959.
- 3.12 General Intelligence Law Amendment Act, Act No. 66 of 2000.
- 3.13 National Strategic Intelligence Act, Act No. 39 of 1994.
- 3.14 Fire-arms Control Act, Act No. 60 of 2000 and regulations.
- 3.15 Protected Disclosures Act, Act No. 26 of 2000.
- 3.16 Prevention and Combating of Corrupt Activities Act, Act No. 12 of 2004.
- 3.17 Public Finance Management Act, Act No.1 of 1999 and Treasury Regulations.
- 3.18 Minimum Information Security Standards (MISS), Second Edition March 1998.
- 3.19 South African Communication Security Agency, SACSA/090/1(4) Communication Security in the RSA.
- 3.20 Proclamation No R 59 of 2009 – establishment of the State Security Agency (SSA).
- 3.21 Intelligence Service Control Act, Act No. 40 of 1994.
- 3.22 National Building Regulations and Building Standards Act, Act No. 103 of 1977.

4. OBJECTIVE

The main objective of this policy is to support the National as well as Provincial interest and the Department of Roads and Public Works' business objectives by protecting employees, information and assets and assuring the continued delivery of services to all South African citizens.

This policy complements other policies of the Department of Roads and Public Works (e.g. the use of laptop computers, losses and damages policy and fraud prevention policy).

This policy seeks to:

- Protect the employees of the Department of Roads and Public Works against identified threats according to baseline security requirements and continuous risk management.
- To secure the information and assets of the Department of Roads and Public Works against identified threats according to baseline security requirements and continuous risk management.
- To ensure the continued delivery of the services of the Department through baseline security requirements, including business continuity planning and continuous risk management.

5. PRINCIPLES, VALUES AND PHILOSOPHY

This policy is intended to reflect the Department's commitment to the principles, goals and ideals described in the departmental vision, mission and core values.

6. SCOPE AND APPLICABILITY

This policy is applicable to all members of the management, employees, consultants, contractors and any other service provider of the Department of Roads and Public Works. It is further applicable to all information assets, intellectual property, fixed and moveable property of the DRPW, visitors and members of the public visiting the premises of or who may officially interact with the institution.

7. PROCEDURES

7.1 Compliance Requirements

All employees of the Department must comply with the baseline security requirements of this policy and its associated Security Directives as contained in the Security Plan of the

Department of Roads and Public Works. These requirements shall be based on integrated security Threat and Risk Assessments (TRA's) in the provincial interest as well as employees, information and assets of the Department of Roads and Public Works. The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.

Security threat and risk assessments involve:

- Establishing the scope of the assessment and identifying the information, employees and assets to be protected.
- Determining the threat to information, employees and assets of the institution and assessing the probability and impact of threat occurrence.
- 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.

7.2 Staff Accountability and Acceptable Use of Assets

The Head of Department shall ensure that the information and assets of the Department are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of the Department of Roads and Public Works.

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

7.3 Specific Baseline Requirements

7.3.1 Security administration

These functions refer to the following:

- 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 security in emergency and increased threat situations.
- Facilitating business continuity planning.
- Ensuring security in contracting.
- Facilitating security breach reporting and investigations.
- Implementation Strategy.

7.4 Security Incident/Breaches Reporting Process

Whenever employees of the institution becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidental or intentional), he/she must report that to the Security Manager of the institution by utilizing the formal reporting procedure prescribed by the Security Breach Directive of the institution.

The Head of Department shall report to the appropriate authority of the institution all cases or suspected cases of security breaches for investigation.

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

7.5 Security Incident/Breaches Response Process

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

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

It shall be the responsibility of the National Intelligence Structures (e.g. the State Security Agency (SSA) or the South African Police Services (SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the institution.

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

The end result of these investigations, disciplinary actions or criminal prosecutions may be taken into consideration by the Head of 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.

7.6 Information Security

7.6.1 Categorization of information and information classification system

The Security Manager must ensure that a comprehensive information classification system is developed for and implemented in the Department. All sensitive information produced or processed in the Department must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure and in accordance with Minimum Information Security Standards (MISS).

All sensitive information must be categorized into one of the following categories:

- State Secret

A state secret consists of information:

- known only to a limited number of people; and
- which ought to be kept secret in order to prevent the safety or interests of the Republic from being endangered.

- Trade Secret

Is any information:

- known only to a limited number of people;
- concerning the commercial or industrial activities of a specific organization or an individual;
- in respect of which the organization or the individual concerned has demonstrated its or his or her desire to keep it secret; and
- which needs to be kept secret in order to protect the economic interests of the state, the organization or the individual concerned.

- Personal Information

Is any information:

- known only to a limited number of people;
- in respect of which the individual has demonstrated his or her desire to keep it private and not to disclose it to the public in general.

- Confidential

Document contains information, referred to in Chapter 4 of the Promotion of Access to Information Act, Act No. 2 of 2000:

- which is a state secret; disclosure would be harmful to the security or interests of the state or could cause embarrassment in its international relations;
- is a trade secret; disclosure of which would cause financial loss to the institution or may cause embarrassment to the institution in its relations with its clients, outside contractors, competitors and suppliers;
- which is personal information; disclosure of which would cause an invasion of the privacy of an individual who is not an employee of the institution, or, in the case of an employee, where the information is information that the institution does not wish its employees in the personnel section should be aware of.

- Secret

Reserved for use in limited circumstances. Document contains information, referred to in Chapter 4 of the Promotion of Access to Information Act, Act No. 2 of 2000:

- which forms a state secret; disclosure of which will endanger security or interest of the state or jeopardize international relations;
- constitutes a trade secret; disclosure of which will cause serious financial loss to the institution.

- Top Secret

Reserved for use in exceptional circumstances.

Document contains information, referred to in Chapter 4 of the Promotion of Access to Information Act, Act No. 2 of 2000:

- which forms a state secret; disclosure will cause serious and irreparable harm to the security or interests of the state or may cause other states to sever diplomatic relations with the Republic;
- constitutes a trade secret; disclosure will cause disastrous results with regard to the future existence of the institution;
- is personal information; disclosure would endanger the life of the individual concerned.

Employees of the institution who generates 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.

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.

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

- Intrinsic secrecy approach.
- Need-to-know.
- Level of security clearance.

7.7 Physical Security

Physical security involves the physical layout and design of facilities of the Department of Roads and Public Works 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 unauthorized access and the activation of an appropriate response. Physical security also includes the provision of measures to protect employees from bodily harm.

Physical security measures must be developed, implemented and maintained in order to ensure that the entire Department of Roads and Public Works, 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.

The Department of Roads and Public Works 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 areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto.
- Include the necessary security specifications in planning, requests for proposals and tender documentation.
- Incorporate related costs in funding requirements for the implementation of the above.

The Department of Roads and Public Works 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. All employees are required to comply with access control procedures of the DRPW at all times.

7.8 Personnel Security

7.8.1 Security screening

All employees, contractors and consultants of the Department of Roads and Public Works, who requires 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) in terms of National Strategic Intelligence Act, Act No.39 of 1994 in order to be granted a security clearance at the appropriate level.

The level of security clearance given to a person will be determined by the contents of or access to classified information entailed by the post already occupied or to be occupied in accordance with their respective responsibilities and accountability.

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

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 of Roads and Public Works.

A security clearance will be valid for a period of ten years in respect of 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 Head of Department of Roads and Public Works based on information which impact negatively on an individual's security competency.

Security clearances in respect of all individuals who have terminated their services with the Department of Roads and Public Works shall be immediately withdrawn.

7.9 Polygraph Screening

A polygraph examination shall be utilized to provide support for the security screening process. All employees subjected to a Top Secret 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.

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.

7.10 Transferability of Security Clearance

A security clearance issued in respect of an official from other government institutions shall not be automatically transferable to the Department of Roads and Public Works. The responsibility for deciding whether the official should be re-screened rests with the Head of Department.

7.11 Security Awareness and Training

A security awareness and training programme must be developed by the Security Manager and implemented to effectively ensure that all personnel and service providers of the Department of Roads and Public Works remain security conscious.

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

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

Regular surveys and walkthrough inspections will be conducted by the Security Manager and members of the security component to monitor the effectiveness of the security awareness and training programme.

7.12 Information and Communication Technology (ICT) Security

7.12.1 Information Technology (IT) security

A security network shall be established for the Department of Roads and Public Works 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.

To prevent the compromise of IT systems, the Department of Roads and Public Works shall implement baseline security controls and any additional controls 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.

To ensure policy compliance, the IT Manager of the Department of Roads and Public Works shall:

- Certify that all IT 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 State Security Agency (SSA) in order to get an independent assessment.

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

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

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

All employees shall make use of the IT systems of the institution in an acceptable manner and for business purposes only. All employees must comply with the IT Security Directives in this regard at all times.

The selection of passwords, their use and management as a primary means of 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.

To ensure the ongoing availability of critical services, the institution shall develop IT continuity plans as part of the overall Business Continuity Planning (BCP) and recovery activities.

7.13. Internet Access

The IT Manager of the Department of Roads and Public Works, having the overall responsibility for setting up Internet access for the Department shall ensure that the network of the institution is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Human Capital 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.

The IT Manager of the institution shall be responsible for controlling user access to the internet, as well as ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security Breaches and incidents.

Incoming e-mail 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.

7.14. Use of Laptop Computers

Usage of laptop computers by employees of the Institution 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.

The information stored on a laptop computer of the institution shall be suitably protected at all times, in line with the protection measures prescribed in the IT Security Directive.

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 Directives.

7.15 Communication Security

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

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

Access to communication security equipment of the institution 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).

7.16 Technical Surveillance Counter Measures (TSCM)

All offices, meeting, conference and boardroom venues of the Department of Roads and Public Works 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 the SSA to ensure that these areas are kept sterile and secure.

The Security Manager of the institution shall ensure that areas that are utilized for discussion of a sensitive nature as well as offices or rooms that house electronic communications equipment such as tape recorders, audio visualsand cellular phones are physically secured in accordance with the standards laid down by the SSA in order to support the sterility of the environment.

No unauthorized electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of the institution is discussed. Authorization must be obtained from the Security Manager / delegated official.

8. BUSINESS CONTINUITY PLAN (BCP)

- The Security Manager (SM) of the DRPW 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 and visitors.

- All employees of the DRPW shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.

9. ROLES AND RESPONSIBILITIES

9.1 The Head of Department

The Head of Department bears the overall responsibility for implementing and enforcing the security programme of the Department. Towards the execution of this responsibility, the Head of Department shall:

- Establish a security committee for the institution and ensure the participation of all the members of senior management, and the members of all the core business functions of the institution in the activities of the committee.
- Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

9.2 The Security Manager

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

- Chair the Security Committee of the institution.
- Draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of the institution in conjunction with the Security Committee.
- Review the Security Policy and Security Plan at regular intervals.
- Conduct a security TRA of the institution with the assistance of the Security Committee.
- Advise management on the security implication of management decisions.
- Implement a security awareness programme.
- Conduct internal compliance audits and inspection at the institution at regular intervals.
- Establish a good working relationship with both the SAPS and the SSA.

9.3 The Security Committee

The Security Committee shall be appointed by the Head of Department. Assisting the Security Manager in the execution of all security related responsibilities of the Department of Roads and Public Works, including completing tasks such as drafting/reviewing of the Security Policy and Security Plan, conducting of security TRA, conducting of security audits, drafting of a Business Continuity Plan and assisting with security awareness and training.

9.4 Programme Managers

All line managers of the Department of Roads and Public Works shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of the institution.

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 warranted.

9.5 Employees, Contractors, Consultants and other Service Providers

Every Employee, Contractor, Consultant and other Service Providers of the Department of Roads and Public Works 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 the institution at all times.

10. ENFORCEMENTS

The Head of Department of Roads and Public Works and the appointed Security Manager are accountable for the enforcement of this policy.

All employees of the institution are required to fully comply with this policy and its associated Security Directives as contained in the Security Plan. Non-compliance with any prescript shall be addressed in terms of the Disciplinary Code/Regulations of the institution.

Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of the institution shall be included in the contracts with such individual(s)/institution(s)/companies. The consequences of any transgression/deviation or non-compliance shall be clearly stipulated in the said contract 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.

11. EXCEPTIONS

Deviations 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 Head of Department (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).

12. OTHER CONSIDERATIONS

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

- Occupational Health and Safety issues of the Department of Roads and Public Works.
- Disaster Management of the Department of Roads and Public Works.
- Disabled people 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.
- Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).

13. COMMUNICATING THE POLICY

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

The Security Manager must ensure that a comprehensive security awareness programme is developed and implemented within the institution to facilitate the above said communication.

Communication of this policy by means of this programme shall be conducted as follows:

- Awareness workshops and briefings to be attended by all employees.

- Distribution of memo's and circulars to all employees.
- Access to the policy and applicable directives on the intranet of the institution.

14. FINANCIAL IMPLICATION

The total projected commitment in terms of this policy is R100 000 per year.

15. MONITORING AND EVALUATION

The Security Manager, with the assistance of the security component and the Security Committee of the Department of Roads and Public Works ensure compliance with this policy and it's associated Security Directives by means of conducting internal security audits and inspection on a frequent basis.

The findings of the said audits and inspections shall be reported to the Head of Department forthwith after completion thereof.

16. DISCIPLINARY ACTION

Any disciplinary action taken in terms of non-compliance with this policy will be in accordance with the disciplinary code/directives of the Department.

17. POLICY REVIEW

This policy shall be assessed annually from the effective date to determine its effectiveness and appropriateness.

18. APPROVALS AND RECOMMENDATIONS

Checked / ~~Not Checked~~

Comments:

.....
.....
.....



STATE SECURITY AGENCY

19 JUNE 2013

DATE:

Recommended / ~~not recommended~~

Comments:

.....
.....
.....



DIRECTOR: LEGAL SERVICES

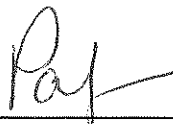
25 June 2013

DATE:

Approved / ~~not approved~~

Comments:

.....
.....
.....



HEAD OF DEPARTMENT

ROADS AND PUBLIC WORKS

NORTHERN CAPE PROVINCE

03/07/2013.

DATE: