



the dr&pw

---

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

# DEPARTMENTAL SECURITY POLICY

Version 9  
(April 2021)

## TABLE OF CONTENTS

<b>Contents</b>	<b>Page</b>
<b>1. DEFINITIONS AND ACRONYMS .....</b>	<b>4</b>
<b>2. INTRODUCTION.....</b>	<b>10</b>
<b>3. BACKGROUND.....</b>	<b>10</b>
<b>4. REGULATORY FRAMEWORK .....</b>	<b>10</b>
<b>5. OBJECTIVE.....</b>	<b>11</b>
<b>6. PRINCIPLES, VALUES AND PHILOSOPHY.....</b>	<b>11</b>
<b>7. SCOPE AND APPLICABILITY .....</b>	<b>12</b>
<b>8. PROCEDURES .....</b>	<b>12</b>
8.1 Compliance Requirements.....	12
8.2 Staff Accountability and Acceptable Use of Assets .....	12
8.3 Specific Baseline Security Requirements .....	13
8.4 Security Incident / Breaches Reporting Process.....	13
8.5 Security Incident / Breaches Response Process.....	13
8.6 Information Security .....	14
8.7 Physical Security.....	16
8.8 Personnel Security.....	17
8.9 Polygraph Screening.....	18
8.10 Transferability of Security Clearance.....	19
8.11 Security Awareness and Training.....	19
8.12 Information and Communication Technology (ICT) Security.....	19
8.13 Internet Access .....	20
8.14 Use of Laptop Computers .....	21
8.15 Communication Security .....	21
8.16 Technical Surveillance Counter Measures (TSCM).....	21
<b>9. BUSINESS CONTINUITY PLAN (BCP).....</b>	<b>22</b>

<b>10. ROLES AND RESPONSIBILITIES .....</b>	<b>22</b>
10.1 Head of Department (HOD).....	22
10.2 Security Manager (SM) .....	22
10.3 Security and Records Management Committee (SRMC) .....	23
10.4 Programme Managers .....	23
10.5 Employees, Contractors, Consultants and other Service Providers.....	23
<b>11. ENFORCEMENTS .....</b>	<b>23</b>
<b>12. EXCEPTIONS.....</b>	<b>24</b>
<b>13. CONSIDERATIONS FOR POLICY IMPLEMENTATION .....</b>	<b>24</b>
<b>14. COMMUNICATING THE POLICY.....</b>	<b>24</b>
<b>15. MONITORING AND EVALUATION (M&amp;E).....</b>	<b>25</b>
<b>16. DISCIPLINARY ACTION.....</b>	<b>25</b>
<b>17. POLICY REVIEW .....</b>	<b>25</b>
<b>18. APPROVAL OF THE POLICY AND DATE OF EFFECT .....</b>	<b>26</b>

## 1. DEFINITIONS AND ACRONYMS

<b>"Access Control"</b>	Refers to the process by which access to a particular area is controlled or restricted to authorised personnel only. This is synonymous with controlled access.
<b>"Accredited"</b>	Means the process of the official authorisation 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.
<b>"Assets"</b>	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.
<b>"BCP"</b>	Means Business Continuity Planning.
<b>"Classification"</b>	Refers to the process whereby all official matters exempted from undue disclosure are labelled Confidential, Secret or Top Secret.
<b>"Contingency Planning"</b>	Refers to 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.
<b>"DDG level"</b>	Refers to Deputy Director General level, which is also applicable to Heads of Department (HODs).

<b>"Declaration"</b>	Means 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.
<b>"Department / DR&amp;PW"</b>	Means Department of Roads and Public Works, Province of the Northern Cape.
<b>"Document"</b>	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.
<b>"Document Security"</b>	Means the application of security measures in order to protect classified / sensitive documents.
<b>"DPSA"</b>	Means Department of Public Service and Administration.
<b>"HOD"</b>	Means the Head of Department (HOD), according to the Public Finance Management Act (PFMA), 1999, who is also the Accounting Officer (AO). The PFMA clarifies the responsibilities of the HOD as Accounting Officer.
<b>"HRM&amp;D"</b>	Means Human Resource Management and Development, which is a directorate of the Department.
<b>"ICT"</b>	Means Information and Communication Technology.
<b>"Information Security"</b>	Means the application of a system to implement personnel, physical, computer, and

	communication security measures to protect sensitive information.
<b>"Internet"</b>	The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP / IP) to serve several billion users worldwide. It is a <i>network of networks</i> that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support e-mail.
<b>"Intranet"</b>	An Intranet is a computer network that uses Internet Protocol (IP) technology to share information, operational systems, or computing services <i>within</i> an organisation.
<b>"M&amp;E"</b>	Means Monitoring and Evaluation. These refer to processes undertaken to monitor and evaluate whether individual departmental units and the Department as a whole are obtaining and utilising their resources effectively and efficiently to accomplish their objectives, and where this is not being achieved, to implement corrective action.
<b>"MEC"</b>	Means Member of the Executive Council, who is the Political Head of the Department (called the "Executive Authority"). The difference between the offices of the Executive Authority and that of the Accounting Officer (HOD) is that the MEC is responsible for policy choices and outcomes, while the HOD takes responsibility for implementing the policy and achieving the outcomes.

<b>"MISS"</b>	Means Minimum Information Security Standards.
<b>"National Intelligence Structures"</b>	Means the National Intelligence Structures as defined in Section 1 of the National Strategic Intelligence Act, Act 39 of 1994.
<b>"OHS"</b>	Means Occupational Health and Safety.
<b>"PAIA"</b>	Refers to the Promotion of Access to Information Act, Act No. 2 of 2000.
<b>"PAJA"</b>	Refers to the Promotion of Administrative Justice Act, Act No. 3 of 2000.
<b>"PERSAL"</b>	Means Personal and Salary Administration System.
<b>"Personnel Security"</b>	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 herself / himself in a manner not exposing her / him or the information to compromise. This could include mechanisms to effectively manage / solve personnel grievances and disciplinary matters.
<b>"PFMA"</b>	Refers to the Public Finance Management Act, Act No.1 of 1999.
<b>"Physical Security"</b>	Refers to that condition which is created by the conscious provision and application of physical security measures for the protection of persons, property and information.
<b>"PSC"</b>	Means Personnel Suitability Check.
<b>"Risk"</b>	Means the likelihood of a threat materialising by

	exploitation of vulnerability.
<b>"SACSA"</b>	Means South African Communication Security Agency.
<b>"SAPS"</b>	Means South African Police Service.
<b>"SATP"</b>	Means Security Awareness and Training Programme.
<b>"SCM"</b>	Means Supply Chain Management.
<b>"Screening Institution"</b>	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.
<b>"Security Audit"</b>	Refers to a process conducted to determine if recommendations made in a previous security assessment has been implemented.
<b>"Security Breach"</b>	Means the negligent or intentional transgression of or failure to comply with security measures.
<b>"Security Clearance"</b>	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.
<b>"SM"</b>	Means Security Manager.
<b>"SRMC"</b>	Means Security and Records Management



	Committee. The SRMC is a departmental committee, with its own Terms of Reference, as approved by the HOD.
<b>"SSA"</b>	Means State Security Agency.
<b>"Threat"</b>	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.
<b>"Threat and Risk Assessment (TRA)"</b>	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.
<b>"TSCM"</b>	Means Technical Surveillance Counter Measures. TSCM is the acronym denoting the process of bug-sweeping or electronic counter surveillance. A TSCM survey is a service provided by qualified personnel to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility. A TSCM survey will provide a professional evaluation of the facility's technical security posture and normally will consist of a thorough visual, electronic, and physical examination in and about the surveyed facility.
<b>"Security Screening / Vetting"</b>	Means the systematic process of investigation followed in determining a person's security competence.

## 2. INTRODUCTION

This policy seeks to protect the employees, information and assets of the DR&PW against identified threats according to baseline security requirements and continuous risk management.

## 3. BACKGROUND

- 3.1 In terms of cabinet approved memoranda, all pre-screening/personnel suitability checks are expected to be conducted by the organs of state themselves. This refers to institutions which have a total workforce that exceeds eight hundred (800) employees in their PERSAL system or establishment.
- 3.2 The DR&PW also falls within this category, and thus has to conduct pre-employment screening of candidates. To this end the Department defers to the instruction from the DPSA, reference number 14/1/1/P, dated 23 November 2007.
- 3.3 The Provincial SSA has since, on numerous occasions informed the Department, by means of screening results, that the Department must take a stand, based on this instruction.

## 4. REGULATORY FRAMEWORK

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

- 4.1 Control of Access to Public Premises and Vehicles Act, Act No. 53 of 1985.
- 4.2 Criminal Procedure Act, Act No. 51 of 1977, as amended.
- 4.3 Private Security Industry Regulations Act, Act No. 56 of 2001.
- 4.4 Protection of Information Act, Act No. 84 of 1982.
- 4.5 Promotion of Access to Information Act (PAIA), Act No. 2 of 2000.
- 4.6 Promotion of Administrative Justice Act (PAJA), Act No. 3 of 2000.
- 4.7 National Archives of South Africa Act, Act No. 43 of 1996.
- 4.8 Occupational Health and Safety Act, Act No. 85 of 1993, as amended.
- 4.9 Constitution of the Republic of South Africa Act, Act 108 of 1996, Section 36.
- 4.10 National Key Points Act, Act No. 102 of 1980.
- 4.11 Trespass Act, Act No.6 of 1959.
- 4.12 General Intelligence Law Amendment Act, Act No. 66 of 2000.
- 4.13 National Strategic Intelligence Act, Act No. 39 of 1994.
- 4.14 Fire-arms Control Act, Act No. 60 of 2000 and regulations.
- 4.15 Protected Disclosures Act, Act No. 26 of 2000.

- 4.16 Prevention and Combating of Corrupt Activities Act, Act No. 12 of 2004.
- 4.17 Public Finance Management Act (PFMA), Act No.1 of 1999 and Treasury Regulations.
- 4.18 Minimum Information Security Standards (MISS), Second Edition March 1998.
- 4.19 South African Communication Security Agency, SACSA/090/1(4) Communication Security in the RSA.
- 4.20 Proclamation No R 59 of 2009 – establishment of the State Security Agency (SSA).
- 4.21 Intelligence Service Control Act, Act No. 40 of 1994.
- 4.22 National Building Regulations and Building Standards Act, Act No. 103 of 1977.
- 4.23 Public service Regulations Act, 2001 (Chapter 1, Part vii, Section B (1) (f); Chapter 5, Part ii, Section B (2)).
- 4.24 Department of Public Service and Administration Circular (DPSA) 14/1/1/P, dated 23 November 2007.
- 4.25 The DR&PW Compilation of Policies on Fraud, Corruption and Ethics Management, called "*The Plan*".

## 5. OBJECTIVE

- 5.1 The main objective of this policy is to support the National as well as Provincial interest and the Department's business objectives by protecting employees, information and assets and assuring the continued delivery of services to all South African citizens.
- 5.2 This policy complements other policies of the DR&PW (e.g. the use of laptop computers, the losses and damages policy and the fraud prevention policy).

### 5.3 This policy seeks to:

- 5.3.1 protect the employees of the DR&PW against identified threats according to baseline security requirements and continuous risk management;
- 5.3.2 secure the information and assets of the DR&PW against identified threats according to baseline security requirements and continuous risk management;
- 5.3.3 ensure the continued delivery of the services of the DR&PW through baseline security requirements, including business continuity planning and continuous risk management.

## 6. 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.

## **7. SCOPE AND APPLICABILITY**

- 7.1 This policy is applicable to all members of the management, employees, consultants, contractors and any other service providers of the DR&PW.
- 7.2 It is further applicable to all information assets, intellectual property, fixed and moveable assets of the DR&PW, visitors and members of the public visiting the premises of or who may officially interact with the Department.

## **8. PROCEDURES**

### **8.1 Compliance Requirements**

- 8.1.1 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 DR&PW.
- 8.1.2 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.
- 8.1.3 The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.
- 8.1.4 Security threat and risk assessments involve:
- a) Establishing the scope of the assessment and identifying the information, employees and assets to be protected.
  - b) Determining the threat to information, employees and assets of the institution and assessing the probability and impact of threat occurrence.
  - c) Assessing the risk based on the adequacy of existing security measures and vulnerabilities.
  - d) Implementing any supplementary security measures that will reduce the risk to an acceptable level.

### **8.2 Staff Accountability and Acceptable Use of Assets**

- 8.2.1 The HOD 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 DR&PW.
- 8.2.2 All employees of the DR&PW shall be accountable for the proper utilisation 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.

### **8.3 Specific Baseline Security Requirements**

#### **8.3.1 Security Administration**

8.3.1.1 These functions refer to the following:

- a) General security administration (departmental directives and procedures, training, and awareness, security risk management, security audits, sharing of information and assets).
- b) Setting of access limitations.
- c) Administration of security screening.
- d) Implementation of physical security.
- e) Ensuring the protection of employees.
- f) Ensuring the protection of information.
- g) Ensuring security in emergency and increased threat situations.
- h) Facilitating business continuity planning.
- i) Ensuring security in contracting.
- j) Facilitating security breach reporting and investigations.
- k) Implementation strategy.

#### **8.4 Security Incident / Breaches Reporting Process**

8.4.1 Whenever employees of the DR&PW becomes aware of an incident that might constitute a security breach or an unauthorised disclosure of information (whether accidental or intentional), he/she must report that to the SM of the Department by utilising the formal reporting procedure prescribed by the Security Breach Directive of the DR&PW.

8.4.2 The HOD shall report to the MEC, who is the Executive Authority of the Department all cases or suspected cases of security breaches for investigation.

8.4.3 The SM of the Department shall ensure that all employees are informed about the procedure for reporting security breaches.

#### **8.5 Security Incident / Breaches Response Process**

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

8.5.2 The SM shall ensure that the HOD is advised of such incidents as soon as possible.

- 8.5.3 It shall be the responsibility of the National Intelligence Structures (e.g. the SSA or the SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the Department.
- 8.5.4 Access privileges to classified information, assets and/or to premises may be suspended by the HOD until administrative, disciplinary and/or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches.
- 8.5.5 The end result of these investigations, disciplinary actions or criminal prosecutions may be taken into consideration by the HOD 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.

## 8.6 Information Security

### 8.6.1 Categorisation of Information and Information Classification System

8.6.1.1 The SM 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, categorised and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure and in accordance with MISS.

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

a) State Secret

A state secret consists of information:

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

b) Trade Secret

Is any information:

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

c) Personal Information

Is any information:

- i) known only to a limited number of people;
- ii) 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.

d) Confidential

Applicable to official documents that contain information referred to in Chapter 4 of the PAIA, Act No. 2 of 2000:

- i) 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;
- ii) 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;
- iii) which is personal information; disclosure of which would cause an invasion of the privacy of an individual who is not an employee of the Department, or, in the case of an employee, where the information is information that the Department does not wish its employees in the HRM&D section should be aware of.

e) Secret

Reserved for use in limited circumstances. Documents in this category contains information, referred to in Chapter 4 of the PAIA, Act No. 2 of 2000:

- i) which forms a state secret; disclosure of which will endanger security or interest of the state or jeopardise international relations;
- ii) constitutes a trade secret; disclosure of which will cause serious financial loss to the Department.

f) Top Secret

Reserved for use in exceptional circumstances. Documents in this category contains information, referred to in Chapter 4 of the PAIA, Act No. 2 of 2000:

- i) 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;
- ii) constitutes a trade secret; disclosure will cause disastrous results with regard to the future existence of the Department;
- iii) is personal information; disclosure would endanger the life of the individual concerned.

8.6.1.3 Employees of the Department who generates sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labelling of classified documents.

8.6.1.4 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.

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

- a) Intrinsic secrecy approach.
- b) Need-to-know.
- c) Level of security clearance.

## **8.7 Physical Security**

8.7.1 Physical security involves the physical layout and design of facilities of the DR&PW and the use of physical security measures to delay and prevent unauthorised 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.

8.7.2 Physical security measures must be developed, implemented and maintained in order to ensure that the entire DR&PW, its personnel, property and information are secured. These security measures shall be based on the findings of the TRA to be conducted by the SM.

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

- 8.7.3.1 select, design and modify facilities in order to facilitate the effective control of access thereto;
- 8.7.3.2 demarcate restricted areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto;
- 8.7.3.3 include the necessary security specifications in planning, requests for proposals and tender documentation; and
- 8.7.3.4 incorporate related costs in funding requirements for the implementation of the above.

8.7.4 The DR&PW 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 DR&PW at all times.



## 8.8 Personnel Security

### 8.8.1 Pre-employment Screening, Vetting and Personnel Suitability Checks (PSC's)

- 8.8.1.1 All pre-screening, vetting and personnel suitability checks are expected to be conducted by the organs of state themselves.
- 8.8.1.2 The above refers to state institutions which have a total workforce exceeding eight hundred (800) employees in their PERSAL system or establishment. The DR&PW falls within this category and is thus required to conduct pre-employment screening of candidates.
- 8.8.1.3 To this end, the Department must comply with the instruction from the DPSA, reference number 14/1/1/P, dated 23 November 2007.
- 8.8.1.4 Pre-employment screening, vetting and security screening of applicants for posts as well as current employed personnel, is considered essential for the protection of classified information.
- 8.8.1.5 Security vetting is a systematic process of investigation followed in determining a person's security competence.
- 8.8.1.6 Pre-screening, utilising PSC's forms will be conducted by security personnel and it will be required when a person is first employed, promoted, transferred or performs general official duties in a post that will give him/her access to classified information.
- 8.8.1.7 The Department will be conducting pre-employment screening to fulfil the mandate of the DPSA and will be monitored in this regard by the SSA.
- 8.8.1.8 All employees, contractors and consultants of the DR&PW 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, in terms of the National Strategic Intelligence Act, Act No.39 of 1994, in order to be granted a security clearance at the appropriate level.
- 8.8.1.9 All staff members, from the lowest level, up to Deputy Director General (DDG) level, who requires access to classified information, must be subjected to security vetting.
- 8.8.1.10 The Department will enforce compliance with a cabinet instruction of 2011 that Supply Chain Management (SCM) personnel, Finance personnel and officials serving in Bid Committees will be subjected to security vetting by the SSA.

- 8.8.1.11 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.
- 8.8.1.12 A security clearance provides access to classified information subject to the need-to-know principle.
- 8.8.1.13 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 DR&PW.
- 8.8.1.14 A security clearance will be valid for a period of ten (10) 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 HOD, based on information which impact negatively on an individual's security competency.
- 8.8.1.15 Security clearances in respect of all individuals who have terminated their services with the DR&PW shall be immediately withdrawn.

## **8.9 Polygraph Screening**

- 8.9.1 A polygraph examination shall be utilised to provide support for the security screening process. All employees subjected to a Top Secret clearance will also be subjected to a polygraph examination.
- 8.9.2 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.
- 8.9.3 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 substantiate his / her honesty concerning questions raised, by making use of the polygraph examination.
- 8.9.4 Refusal by the applicant to undergo the examination does not necessarily signify that a security clearance will not be granted.

## **8.10 Transferability of Security Clearance**

- 8.10.1 A security clearance issued in respect of an official from other government departments / institutions shall not be automatically transferable to the DR&PW.
- 8.10.2 The responsibility for deciding whether the official should be re-screened rests with the HOD.

## **8.11 Security Awareness and Training**

- 8.11.1 A Security Awareness and Training Programme (SATP) must be developed by the SM and implemented to effectively ensure that all personnel and service providers of the DR&PW remain security conscious.
- 8.11.2 All employees shall be subjected to the security awareness and training programmes and must acknowledge in writing, that the contents of the programme(s) has been understood and will be complied with.
- 8.11.3 The programme must cover training with regard to specific security responsibilities and sensitise employees and relevant contractors and consultants about the Security Policy and security measures of the DR&PW and the need to protect sensitive information against disclosure, loss or destruction.
- 8.11.4 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.
- 8.11.5 Attendance of the above programmes is compulsory for all employees identified and notified to attend the events.
- 8.11.6 Regular surveys and walk-through inspections will be conducted by the SM and members of the security component to monitor the effectiveness of the security awareness and training programme.

## **8.12 Information and Communication Technology (ICT) Security**

- 8.12.1 A security network shall be established for the DR&PW 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.
- 8.12.2 To prevent the compromise of departmental ICT systems, the DR&PW 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.

- 8.12.3 To ensure policy compliance, the Manager responsible for the ICT systems of the Department shall:
- a) certify that all ICT systems are secure after procurement, accredit ICT systems prior to operation and comply with minimum security standards and directives;
  - b) conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis; and
  - c) periodically request assistance, review and audits from the SSA in order to get an independent assessment.
- 8.12.4 Server rooms and other related security zones where ICT equipment are kept shall be secured with adequate security measures and strict access control shall be enforced and monitored.
- 8.12.5 Access to the resources on the network of the Department shall be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals of the Department shall be restricted unless explicitly authorised.
- 8.12.6 System hardware, operating and application software, the network and communication systems of the Department shall all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion.
- 8.12.7 All employees shall make use of the ICT systems of the Department in an acceptable manner and for departmental business purposes only. All employees must comply with the ICT Security Directives in this regard at all times.
- 8.12.8 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 ICT Security Directives; in particular, passwords shall not be shared with any other person for any reason.
- 8.12.9 To ensure the ongoing availability of critical services, the institution shall develop ICT continuity plans as part of the overall BCP and recovery activities.

### **8.13. Internet Access**

- 8.13.1 The Manager responsible for ICT systems of the DR&PW, having the overall responsibility for setting up Internet access for the Department, shall ensure that the network of the Department is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall.

**DEPARTMENTAL SECURITY POLICY**

8.13.2 HRM&D 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.

8.13.3 The ICT Manager of the Department 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.

8.13.5 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.

**8.14. Use of Laptop Computers**

8.14.1 Usage of laptop computers by employees of the DR&PW is restricted to business purposes only, and users shall be made aware of, and abide by, the terms and conditions of use, especially the responsibility for the security of information held on such devices.

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

8.14.3 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.

**8.15 Communication Security**

8.15.1 The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of the DR&PW in all its forms and at all times.

8.15.2 All sensitive electronic communication by employees, contractors or employees of the Department must be encrypted in accordance with the SACSA standards, and the Communication Security Directives of the Department. Encryption devices shall only be purchased from SACSA and will not be purchased from commercial suppliers.

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

**8.16 Technical Surveillance Counter Measures (TSCM)**

8.16.1 All offices, meeting, conference and boardroom venues of the DR&PW, 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.

8.16.2 Periodic electronic TSCM (sweeping) will be conducted by the SSA to ensure that these areas are kept sterile and secure.

8.16.3 The SM of the Department shall ensure that areas that are utilised for discussion of a sensitive nature, as well as offices or rooms that house electronic communications equipment such as tape recorders, audio-visual equipment and cellular phones, are physically secured in accordance with the standards laid down by the SSA in order to support the sterility of the environment.

8.16.4 No unauthorised electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of the Department is discussed. Authorisation must be obtained from the SM or a delegated official.

## **9. BUSINESS CONTINUITY PLAN (BCP)**

9.1 The SM of the DR&PW must establish a BCP to provide for the continued availability of critical services, information and assets if a threat materialises and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of employees, contractors' consultants and visitors.

9.2 All employees of the DR&PW shall be made aware of, and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.

## **10. ROLES AND RESPONSIBILITIES**

### **10.1 Head of Department (HOD)**

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

- a) establish a Security and Information and Communication Technology Committee (SRMC) for the Department and ensure the participation of all the members of Senior Management, and the members of all the core business functions of the DR&PW in the activities of the committee; and
- b) approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

### **10.2 Security Manager (SM)**

10.2.1 The delegated security responsibilities lies with the SM of the DR&PW, who will be responsible for the execution of the entire security function and programme of the Department

(coordination, planning, implementation, controlling, etc.). Towards the execution of his/her responsibilities, the SM shall, amongst others:

- a) draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of the Department in conjunction with the SRMC;
- b) review the departmental Security Policy and Security Plan at regular intervals;
- c) conduct a security TRA of the Department, with the assistance of the SRMC;
- d) advise management on the security implications of management decisions;
- e) implement a security awareness programme;
- f) conduct internal compliance audits and inspection at the Department at regular intervals;  
and
- g) establish a good working relationship with both the SAPS and the SSA.

### **10.3 Security and Records Management Committee (SRMC)**

10.3.1 The SRMC shall be appointed by the HOD and operate in accordance with its Terms of Reference, as approved by the HOD.

10.3.2 The SRMC shall assist the SM in the execution of all security related responsibilities of the DR&PW, including completing tasks such as drafting/reviewing of the departmental Security Policy and Security Plan, conducting of security TRA's, conducting of security audits, drafting of a Business Continuity Plan (BCP) and assisting with security awareness and training.

### **10.4 Programme Managers**

10.4.1 All line managers of the DR&PW shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of the Department.

10.4.2 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 warranted.

### **10.5 Employees, Contractors, Consultants and other Service Providers**

Every employee, contractor, consultant and service provider of the DR&PW 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 Department at all times.

## **11. ENFORCEMENTS**

11.1 The HOD of the DR&PW is accountable for the enforcement of this policy.



- 11.2 All employees of the Department 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 Department and the Public Service.
- 11.3 Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of the Department shall be included in the contracts with such individual(s) / institution(s) / companies.
- 11.4 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.

## **12. EXCEPTIONS**

- 12.1 Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:
- 12.1.1 when security must be breached in order to save or protect the lives of people;
- 12.1.2 during unavoidable emergency circumstances e.g. natural disasters;
- 12.1.3 in accordance with written permission from 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).

## **13. CONSIDERATIONS FOR POLICY IMPLEMENTATION**

- 13.1 The following shall be taken into consideration when implementing this policy:
- 13.1.1 The departmental Occupational Health and Safety (OHS) policy and OHS-related issues of the DR&PW.
- 13.1.2 Disaster Management Directives of the DR&PW.
- 13.1.3 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.
- 13.1.4 Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).

## **14. COMMUNICATING THE POLICY**

- 14.1 The SM of the DR&PW, with the assistance of the departmental Communication and Marketing Unit, where necessary, 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 Department.

- 14.2 The SM will further ensure that all security policy and security directive prescriptions are enforced and complied with.
- 14.3 The SM must ensure that a comprehensive security awareness programme is developed and implemented within the Department to facilitate the above said communication.
- 14.4 Communication of this policy shall be conducted as follows:
  - 14.4.1 awareness workshops and briefings to be attended by all employees;
  - 14.4.2 distribution of memo's and circulars to all employees; and
  - 14.4.3 access to the policy and applicable directives on the Intranet of the Department.

## **15. MONITORING AND EVALUATION (M&E)**

- 15.1 The SM, with the assistance of the security component, the SRMC and the Monitoring and Evaluation (M&E) unit of the Department are to ensure compliance with this policy and its associated Security Directives by means of conducting internal security audits and inspection on a frequent basis.
- 15.2 The findings of the said audits and inspections shall be reported to the HOD 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 and the Public Service.

## **17. POLICY REVIEW**

- 17.1 The assessment to determine the effectiveness and appropriateness of this policy will be done five (5) years after its effective date. The assessment could be performed earlier than five (5) years to accommodate any substantial structural or other organizational changes at the Department or any change required by law.
- 17.2 The policy shall be reviewed to specifically factor in changes in legal frameworks, organisational development, political and economic trends, as well as the outcomes of monitoring and evaluation processes.

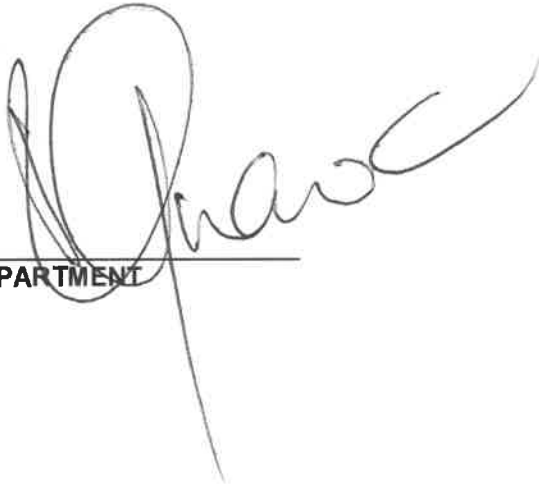
17.3 Deviations from this policy must be approved by the HOD.

**18. APPROVAL OF THE POLICY AND DATE OF EFFECT**

This policy is Approved / ~~Not Approved~~

Comments:

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



\_\_\_\_\_  
HEAD OF DEPARTMENT

29.04.2021  
DATE



**the dr&pw**

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

## INTERNAL MEMO

<b>DATE:</b>	15 APRIL 2021	<b>REF. NO.</b>	
<b>TO:</b>	THE DIRECTOR: STRATEGIC PLANNING MANAGEMENT		
<b>FROM:</b>	THE DEPUTY DIRECTOR: POLICY AND RESEARCH MANAGEMENT SERVICES		
<b>SUBJECT:</b>	<b>SUBMISSION FOR APPROVAL OF REVIEWED DEPARTMENTAL POLICY DOCUMENTS</b>		

Dear Ms. Bekebeke

Please find attached the final drafts of the reviewed departmental policy documents on Security; Contract Management; the Monitoring and Evaluation (M&E) Framework; and the Registry Manual on Procedures at Registry for your perusal and consideration. The above mentioned policy documents have been circulated departmentally for consultation and inputs for review, and it is hereby submitted for approval by the Acting Head of Department (HOD).

Regards,

Mr. T. Ferreira  
Manager: Policy and Research Management Services



**the dr&pw**

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

## INTERNAL MEMO

<b>DATE:</b>	15 APRIL 2021	<b>REF. NO.</b>	
<b>TO:</b>	THE HEAD OF DEPARTMENT (HOD)		
<b>FROM:</b>	THE DIRECTOR: STRATEGIC PLANNING MANAGEMENT		
<b>COPY:</b>	THE CHIEF DIRECTOR: CORPORATE AND MANAGEMENT SERVICES		
<b>SUBJECT:</b>	<b>SUBMISSION FOR APPROVAL OF REVIEWED POLICIES</b>		

### Purpose

1. The purpose of this submission is to obtain approval from the Acting Head of Department (HOD) for the operationalization within the Department of the following reviewed departmental policy documents:

- ✚ Security Policy;
- ✚ Contract Management Policy;
- ✚ Monitoring and Evaluation Policy Framework; and
- ✚ Registry Manual on Procedures at Registry.

### Recommendations

1. The above mentioned reviewed policy documents have been circulated departmentally by the Communication and Marketing Unit to consult the staff members in order to provide an opportunity for inputs toward the review of said policy documents.

**SUBMISSION FOR APPROVAL OF REVIEWED DEPARTMENTAL  
POLICY DOCUMENTS**

2. It is therefore recommended that the Acting HOD approve these reviewed versions of these policy documents as Departmental policy.
  
3. Please see e-mails attached of the Evidence of Departmental Consultation.



MS. B. BEKEBEKE  
DIRECTOR: STRATEGIC PLANNING MANAGEMENT  
Recommended / Not Recommended

21/04/2021  
DATE



MS. A. MPOTSANG  
CHIEF DIRECTOR: CORPORATE AND MANAGEMENT SERVICES  
Recommended / Not Recommended

2021-04-28  
DATE



MS. R. GREWAN  
ACTING HEAD OF DEPARTMENT  
Policies Approved / Policies Not Approved

29.04.2021  
DATE



the dr&pw

---

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

**EVIDENCE OF CONSULTATION WITH  
DEPARTMENTAL STAKEHOLDERS**

**REVIEWED DEPARTMENTAL POLICIES  
ON:**

- 🚧 SECURITY;**
- 🚧 CONTRACT MANAGEMENT;**
- 🚧 MONITORING AND EVALUATION (M&E)  
FRAMEWORK; AND**
- 🚧 REGISTRY MANUAL ON PROCEDURES AT  
REGISTRY.**

**SUBMISSION FOR APPROVAL  
15 APRIL 2021**

**T Ferreira - REVIEW OF SECURITY POLICY**

**From:** DRPW-Info

**To:** A AMokwadi; A Maina; A van Staden; ABrand; ACLouw; AFembers; AKula; ALesotho; ALSishi; AMasisi; AMiller; AMkhize; AMoeti; AMofokeng; AMotlagodisa; Andre Jooste; Andrew Pulen; Anne AMPotsang; APulen; ARudman; ASwanepoel; AvanHeerden; B BDamon; BaatileItumeleng; Babalwa Bekebeke; BBarends; BBobeje; BChotelo; BCloete; BGaonakala; BKapanda; BMazwi; BMeruti; BMontshiwa; BonoloMakoko; BosmanP; Bradley Slingers; BSedisho; BSemau; BSlingers; BValentine; C CvanRooi; C Robertson; CAbrahams; CAdams; CBailey; CChakela; CDenysschen; CFourie; ChanelFourie; ChantelleCloete; ChristinaF; CKakora; Clive Bailey; CMrwebi; CNdebele; CRabaji; CRöbertson; CValentine; D DMokoena; D DMwembo; DBingwa; DBingwane; Denice Bingwane; DGaehete; DKowa; DMAqutyana; DMAqutyana; DMokgatlhe; DMonyamane; DPhirisi; DRPW-Info; DRPW-Switchboard; DSolo; DTsoai; DvdMerwe; EbenSwartbooi; EBeukes; EBreytenbach; Ed Simon; EduPlessis; Edward Simon; EJonkers; EKhatwane; ELecwedi; Ella Modise; EMichaels; ENodoba; EPino; EricksenA; ESimon; FDooling; FMogoje; FPetoro; FvanVuuren; GAppels; Garnett Keyser; GCloete; GJacobs; Gladwyn Stuurman; GMoabi; GMolale; GNakana; GPietersen; GPino; GSalimana; GSefotho; GThupe; GTopkin; Harold Roberts; Henry De Wee; HPuley; HvanderMerwe; I Bulane; IICarolus; IIThopile; I MichaelsI; IFridericks; I Lottering; IMolore; IOliphant; IRammutla; Isaac Prins; J Esterhuyse; J JHanekom; JillianWilliams; JMarx; JMhlongo; JMhlongo; JMolale; JMoncho; JSehume; JSeptember; JSibiya; JSitler; JSpetember; JTawine; June Erasmus; K KMaarman; K KMatonkonyane; K MalgasK; KAaron; KagishoModise; KatzS; KBeuzana; KBopape; KChomi; KDennis; KERicksen; KHenyekane; KKgomo; KKross; KLawrence; KLeboko; KLeserwane; KNdaba; KPike; KPMogorosi; KRifles; KrugerS; KSegwai; L AnthonyL; L Libang; L LleBreton; L LSeobi; L Molemal; LATwell; LawrenceM; LBuffel(...)

**Date:** 3/15/2021 11:56 AM

**Subject:** REVIEW OF SECURITY POLICY

**Attachments:** DEPARTMENTAL SECURITY POLICY Version 8.docx

Good day Colleagues

Kindly find the attached DR&PW's departmental Security Policy, which is under review. The due date for inputs/feedback from staff members is Monday, 22 March 2021 and inputs can be e-mailed to [tferreira@ncpg.gov.za](mailto:tferreira@ncpg.gov.za).

Thank you



DRPW-info@ncpg.gov.za  
**COMMUNICATION AND MARKETING SERVICES**

Stay informed by logging on to the following links



[ncprw.ncpg.gov.za](http://ncprw.ncpg.gov.za)



<https://www.facebook.com/NCdrpw>



@NC\_drpw

Department of Roads and Public Works

Tebogo Leon Tume Complex  
9-11 Stokroos Street  
Squarehillpark  
Kimberley  
8301

Tel: 053 839 2100  
Fax: 053 8392290

**Trendsetters in infrastructure delivery to change the economic landscape of the province'**