the dr&pw

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

DEPARTMENTAL POLICY ON SECURITY BREACHES

Version 2

(April 2021)

TABLE OF CONTENTS

Contents **Page**

1. DEFINITIONS AND ACRONYMS

"COMSEC"	Means Electronic Communication Security (PTY) LTD.
"Cryptography"	It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.
"Department (DR&PW)"	Means Department of Roads and Public Works, Northern Cape Province.
"Document Security"	Means the application of security measures in order to protect classified / sensitive documents.
"Encryption"	It is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties.
"HOD"	Means Head of Department (DR&PW).
"Information Security"	Means the application of a system to implement personnel, physical, computer, and communication security measures to protect sensitive information.
"Institution"	Refers to an institution of state, in this case the Department of Roads and Public Works, Northern Cape Province.
"M&E"	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.
"National Intelligence Structures"	Means the National Intelligence Structures as defined in Section 1 of the National Strategic Intelligence Act, Act 39 of 1994.
"PAIA"	Refers to the Promotion of Access to Information Act, Act No. 2 of 2000.
"PAJA"	Refers to the Promotion of Administrative Justice Act, Act No. 3 of 2000.
"PFMA"	Refers to the Public Finance Management Act, Act No.1 of 1999.

"SAPS"	Means South African Police Service.
"SANDF"	Means South African National Defence Force.
"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"	That condition free of danger created by the conscious provision and application of security measures.
"Security audit"	Refers to a process conducted to evaluate the effectiveness and application of security policy/standards and procedures and to make recommendations for improvement where necessary.
"Security breach"	Means the negligent or intentional transgression of or failure to comply with security measures.
"SRMC"	Means Security and Records Management Committee, which is a departmental structure.
"SM"	Means Security Manager.
"SSA"	Means State Security Agency.
"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.

2. INTRODUCTION

This departmental policy on security breaches has been formulated in order to review the manner in which the security breach is conducted and to inform all officials (including consultants, contractors and interns) employed by this Department, of the procedure put in place in order to manage security breaches at the workplace.

3. REGULATORY FRAMEWORK

3.1 The Criminal Procedure Act, Act No. 51 of 1977, as amended.
3.2 The Protection of Information Act, Act No. 84 of 1982.
3.3 The Promotion of Access to Information Act (PAIA), Act No. 2 of 2000.
3.4 The Promotion of Administrative Justice Act (PAJA), Act No. 3 of 2000.
3.5 The National Archives of South Africa Act, Act No. 43 of 1996.
3.6 The Occupational Health and Safety Act, Act No. 85 of 1993, as amended.
3.7. The Constitution of the Republic of South Africa, Act 108 of 1996, Section 36
3.8. The Prevention and Combating of Corrupt Activities Act, Act No. 12 of 2004.
3.9. Section 38(1)(a)(i) of the Public Finance Management Act (PFMA), Act No.1 of 1999 and Treasury Regulations.
3.10 The Minimum Information Security Standards (MISS), Second Edition, March 1998.

4. INVESTIGATION OF SECURITY BREACHES

4.1 All security breaches or suspected security breaches must be investigated in order to:

4.1.1 Determine:

a) whether a breach did occur and which factors constituted the breach;
b) how and when the breach occurred;
c) what items or information was affected (lost, damaged, compromised);
d) who committed the breach;
e) why the breach occurred (what caused it, what was the purpose or aim of the perpetrator); and
f) which security measures were bypassed or circumvented and how that happened.

4.1.2 Assess the damage that was caused or possibly caused.

4.1.3 Make recommendations regarding steps to be taken to prevent a re-occurrence of the breach.

4.2 The head of an institution or his / her delegate must report to the appropriate authority (as indicated in Section 2 of the National Strategic Intelligence Act, 39 of 1994), all cases or suspected cases of security breaches that must be investigated.

4.3 Heads of institutions must ensure that all staff members are informed about the procedure by means of an internal security awareness program. The SSA security advisers are available for guidance and advice in this regard.

5. THE ROLES OF THE VARIOUS MEMBERS OF THE NATIONAL INTELLIGENCE STRUCTURES WITH REGARD TO REPORTING AND INVESTIGATION OF SECURITY BREACHES

5.1 The Role of the State Security Agency (SSA)

5.1.1 In terms of Section 2(1) (b) of the National Strategic Intelligence Act; Act No. 39 of 1994, the SSA shall fulfil the national counter-intelligence responsibilities and for the purpose to conduct and co-ordinate counter-intelligence and to gather, correlate, and evaluate in order to supply intelligence relating to any such threat to the SAPS for the purpose of investigating an offence or alleged offence.

5.1.2 Once a security breach has occurred and it also constitutes the commission of a criminal offence, the information should be conveyed without delay to the SAPS for a court directed investigation of the alleged offence.

5.2 The Role of the South African Police Service (SAPS)

5.2.1 The SAPS is responsible for counter-intelligence measures within the ambit of the SAPS, in terms of Section 2 of the National Strategic Intelligence Act (39 of 1994). This involves the monitoring by the SAPS of compliance with relevant legislation, National Security Standards and internal security policy.

5.2.2 The role of the SAPS in respect of all security breaches, which might amount to a criminal offence, is that of court directed investigation. This is irrespective of whether it has occurred in one of the intelligence structures or any other Department of the State. These include all suspected or alleged security breaches, which could amount to an offence. Therefore all such cases must be reported to the SAPS for investigation with the view of prosecuting them.

5.2.3 Intelligence and information at the disposal of the SAPS, which indicates a counter-intelligence threat or incident in the environment of an institution other than the SAPS, must be forwarded to the SSA without delay.

5.3 The Role of the State Security Agency (SSA) (Foreign Branch)

5.3.1 The role of the SSA (Foreign Branch) is similar to that of the SANDF although it includes South African missions abroad. In cases of security investigations at missions abroad, the findings must be reported to the SSA (Domestic Branch) and the affected department.

6. PROCEDURE TO BE FOLLOWED FOR REPORTING OF BREACHES

6.1 Whenever an official of an institution of state becomes aware of an incident that might constitute a security breach or unauthorized disclosure of information (whether accidentally or intentionally) he/she should report that to the institution's SM.

6.2 The SM should assess whether the incident is intentional and criminal in nature or whether it constitutes purely a possible accidental security breach, or whether it is a case of a mixture of both, in order to ensure that the incident is reported to the correct institution. He /she must also determine whether cryptographic equipment was involved.

6.3 Cases which is of a criminal nature, must immediately be reported to the nearest SAPS station by the SM.

6.4 Where the case has elements of both a criminal offence and a breach of security, e.g. theft of a laptop computer), the matter should be reported to both the SAPS and the SSA.

6.5 If it constitutes a breach of security only, it must be reported to SSA.

6.6 If cryptographic equipment was involved, the case must be reported to both the SSA and COMSEC. If COMSEC determines that an algorithm was compromised, it will notify all affected institutions that utilized the same algorithm. In cases where cryptographic equipment was stolen, the matter must be reported to the SAPS.

6.7 When a security breach is reported to the SSA, it must be reported directly to the security advisor assigned to that institution. For this purpose *inter alia*, all institutions have been and are provided with the contact particulars of the security advisors. If the assigned security advisor is unavailable to assist for any reason, the case(s) may be reported to the SSA Alert Centre. All telephonic reports of such cases must be followed up in writing, addressed to the Provincial Head of the SSA or General Manger: Vetting and Advising.

6.8 The security advisor will immediately respond to the report by arranging a meeting between the investigator and the institution in order to determine the exact nature of the security breach and whether further investigation of the matter falls within the legal mandate of the SSA. If it is established that an SSA investigation should be conducted, the investigator can immediately commence with such an investigation, while the advisor can provide advice about immediate steps that should be taken to limit the damage and security measures that need to be implemented.

6.9 The institution will at that stage be requested to report the incident in writing (if the initial report has been verbal) to the SSA. This report must contain a brief description of the incident and the type of security breach that occurred, reasons for requesting an investigation into the matter as well as relevant contact particulars. The security advisor will provide to the investigator all relevant information, including an outline of security advice and recommendations that had been provided and made to the institution prior to the incident.

6.10 The SSA security advisers will render further assistance during the course of the investigation (if and when required).

6.11 The SSA security investigators must make an assessment at the commencement of the investigation, whether the investigation should be court directed and must involve co-ordination with SAPS from the outset. In instances where an SSA and SAPS investigation may be conducted concurrently or jointly, both SSA and SAPS investigators should ensure proper coordination with regard to the matter with each other.

6.12 After the investigation has been completed, a feedback report on the matter is forwarded to the institution. The report will contain the findings (all relevant information with regard to the perpetrator(s), contributing factors and security deficiencies) and recommendations for the incident and the improvement of security.

6.13 SSA security advisers will advise the institution on security deficiencies that might have contributed to the breach of security.

6.14 All institutions must implement an internal control mechanism for the reporting of security breaches. Implementing a register where all breaches of security at the institution must be registered could facilitate this. This would facilitate better control with regard to the monitoring of progress and the outcome of investigations into security breaches (both internally and during security audits conducted by the SSA).

7. ENFORCEMENT OF THE POLICY

7.1 The HOD of the DR&PW and the appointed SM are accountable for the enforcement of this policy.

7.2 All employees of the DR&PW are required to fully comply with this policy and its associated Security directives. Non-compliance with any prescript shall be addressed in terms of the Disciplinary Code/Regulations of the DR&PW and the Public Service.

7.3 These policy prescripts are to be fully complied with by all consultants, contractors or service providers of the DR&PW. The consequences of any transgression/deviation or non-compliance

shall be strictly enforced. Such consequences may include disciplinary action or termination of the service or contract, depending on the nature of any non-compliance.

8. EXCEPTIONS

8.1 Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:

8.1.1 When security must be breached in order to save or protect the lives of people.

8.1.2 During unavoidable emergency circumstances e.g. natural disasters.

8.1.3 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. COMMUNICATING THE POLICY

9.1 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.

9.2 The SM will further ensure that all security policy and security directive prescriptions are enforced and complied with.

9.3 The SM must ensure that a comprehensive security awareness programme is developed and implemented within the Department to facilitate the above said communication.

9.4 Communication of this policy shall be conducted as follows:

9.4.1 awareness workshops and briefings to be attended by all employees;

9.4.2 distribution of memo's and circulars to all employees; and

9.4.3 access to the policy and applicable directives on the Intranet of the Department.

10. MONITORING AND EVALUATION (M&E)

10.1 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 it's associated Security Directives by means of conducting internal security audits and inspection on a frequent basis.

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

11. 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.

12. POLICY REVIEW

12.1 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.

12.2 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.

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

13. APPROVAL OF THE POLICY AND DATE OF EFFECT

This policy is Approved / ~~Not Approved~~

Comments:

.....

.....

.....

.....

HEAD OF DEPARTMENT

20/04/21
DATE

the dr&pw

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

INTERNAL MEMO

DATE:	08 APRIL 2021	**REF. NO.**	
TO:	THE DIRECTOR: STRATEGIC PLANNING MANAGEMENT		
FROM:	THE DEPUTY DIRECTOR: POLICY AND RESEARCH MANAGEMENT SERVICES		
SUBJECT:	**SUBMISSION FOR APPROVAL OF REVIEWED DEPARTMENTAL POLICY DOCUMENTS**		

Dear Ms. Bekebeke

Please find attached the final drafts of the reviewed departmental policy documents on Banking and Cash Management; Revenue Management; Gifts and Donations; Security Breaches; and Sport and Recreation, for your perusal and consideration. The above mentioned policy documents has 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

EVIDENCE OF CONSULTATION WITH DEPARTMENTAL STAKEHOLDERS

REVIEWED DEPARTMENTAL POLICIES ON:

- BANKING AND CASH MANAGEMENT;
- REVENUE MANAGEMENT;
- GIFTS AND DONATIONS;
- SECURITY BREACHES; AND
- SPORT AND RECREATION.

SUBMISSION FOR APPROVAL
08 APRIL 2021

TFerreira - REVIEW of Policy on Security Breaches

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; CRobertson; 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; GSefotlho; GThupe; GTopkin; Harold Roberts; Henry De Wee; HPuley; HvanderMerwe; I Bulane; I ICarolus; I ITlhopile; I MichaelsI; IFredericks; ILottering; 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 10:36 AM

Subject: REVIEW of Policy on Security Breaches

Attachments: Approved DR&PW Policy on Security Breaches - Ver 1 - Oct 2016.pdf

Good day Colleagues

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

Thank you

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

Stay informed by logging on to the following links

ncrpw.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'