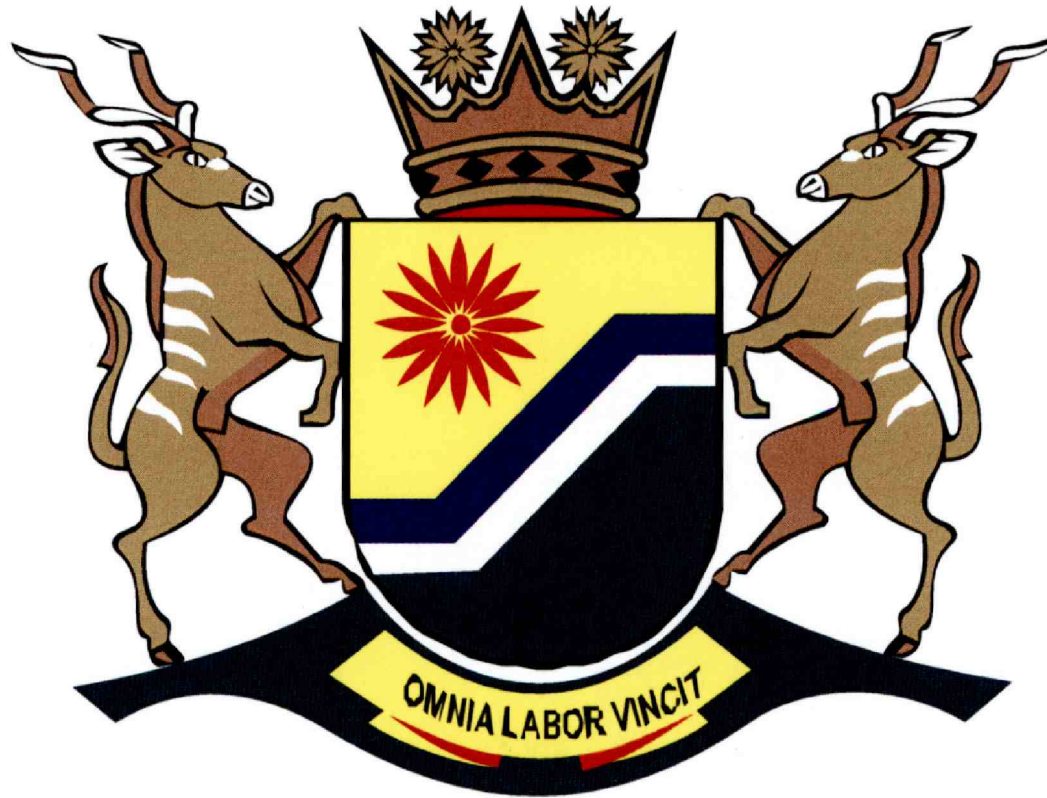


Mpumalanga Provincial Government



Department of Public, Works Roads and Transport

SECURITY POLICY

Revision Date:.....	None
Issue:	1.0
Responsible Section.....	Human Resource Planning
Approval Date.....	

TABLE OF CONTENTS

Item/ Topic	Pages
Abbreviations and Definitions	3
1. Introduction	4
2. Objectives	4
3. Regulatory Framework	4
4. Scope of Application	5
5. Policy Statement	5 - 8
6. Roles and Responsibilities	8
7. Monitoring	9
8. Policy Review	9
9. Approval	9

ABBREVIATIONS

MEC: Member of the Executive Council
HOD: Head of Department
SMS: Senior Management Services
MMS: Middle Management Services
PSR: Public Service Regulation
MISS: Minimum of Information Security Services
NIA: National Intelligence Agency
SM: Security Manager
SAPS: South African Police Service

1. DEFINITIONS

Security Policy - formal statements of the rules through which people are given access to an institution's assets.

Security Principles - Foundation upon which security policies can be further developed.

Security Procedures - Specific interpretation of the security policy to instruct people on how to implement the policy.

Top Secret-Classification - information that can be used by enemies or hostile/malicious elements to neutralize the objectives and functions of state/institutions

Secret-classification - information that may be used by hostile/opposing/malicious elements to disrupt the objectives and functions of state or an institution

Confidential-Classification - information that may be used by hostile/opposing/malicious elements to harm the objectives and functions of an individual or an institution

Department - Department of Public Works, Roads and Transport

State Property - Immovable and movable assets of the Department of Public Works, Roads and Transport.

2. INTRODUCTION

The Department of Public Works, Roads and Transport shall ensure safety and security of its assets against the potential threats. These includes, internal, external, manmade and natural, which may have negative effect on the Departments effectiveness to deliver on its mandate. Should these threats not be controlled/managed properly the state security could be compromised.

3. OBJECTIVES

The main objective of this policy is to protect national interest and the Department of Public Works, Roads and Transport business objectives by supporting employees, information and assets as well as assuring the continued delivery of services to South African Citizens. This policy complements other departmental policies (e.g. Safety, Health, Environment and Quality Management Policy, Records Management Policy, Asset Management Policy, Immovable and Supply Chain Policy) that are aimed at safeguarding information, employees and assets of the Department.

4. REGULATORY FRAMEWORK

- 4.1 Constitution of Republic of South Africa, 1996
- 4.2 Public Service Act, 1994
- 4.3 Public Service Regulation, 2001
- 4.4 Promotion of Access to information Act, 2 of 2000
- 4.5 Electronic Communication and Transactions Act, 25 of 2002
- 4.6 Interception of Communications and provision of Communication-Related
- 4.7 Information Act, 70 of 2002
- 4.8 Criminal Procedure Act 51 of 1977
- 4.9 Private Security Industry Regulatory Authority Acts 57 of 2000
- 4.10 Control of Access to Public Premises and Vehicles Act 53 of 1985
- 4.11 Occupational Health and Safety Act 85 of 1993
- 4.12 Protection of Information Act 84 of 1982
- 4.13 Trespass Act 6 of 1959
- 4.15 National Archives Act 43 of 1996
- 4.16 Public Finance Management Act 1 of 1999
- 4.17 Fire Brigade Act 99 of 1987
- 4.18 Basic Conditions of Employment Act 75 of 1997
- 4.19 Compensation for Occupational Injuries and Disease Act 61 of 1997
- 4.20 Firearms Control Act 60 of 2000
- 4.21 Arms and Ammunition Act 75 of 1969
- 4.22 Civil Protection Act 67 of 1977
- 4.23 Labour Relation Act 66 of 1995
- 4.24 Skills Development Act 97 of 1998
- 4.25 Intelligence Service Act 38 of 1994
- 4.26 Justice of the Peace and Commissioners of Oaths Act 16 of 1963
- 4.27 Minimum Information Security Standard

5. SCOPE OF APPLICATION

The policy shall apply to all Security Services within the Department, personnel, contractors, consultants and all stakeholders.

6. POLICY STATEMENT

6.1 CATEGORIES OF SECURITY

6.1.1 PERSONNEL SECURITY

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

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

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

6.1.1.3 A declaration of secrecy shall be signed by every individual issued with a security clearance to complement the entire security screening process. This shall remain valid even after the individual has terminated his/her services with the department.

6.1.1.4 A security clearance shall be valid for a period of ten years in respect of the confidential level and five years for Secret and Top Secret. This does not preclude re-screening at a more frequent basis as determined by the Head of Department, based on information which impact negatively on an individual's security competence.

6.1.2 DOCUMENT SECURITY

The Department shall ensure that all documents in its possession and under control are classified in accordance with the levels set out in the MISS document to prevent inadvertent disclosure. This includes departmental records which shall be managed and disposed as per the National Archives Act.

6.1.2.2 Categorization of information and information classification system

6.1.2.1.1 The Security Manager(SM) shall ensure that a comprehensive information classification system is developed for and implemented in the department. All sensitive information produced or processed by the department shall be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.

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

- 6.1.2.2.1 State Secret
- 6.1.2.2.2 Trade Secret; and
- 6.1.2.2.3 Personal Information

6.1.2.3 And subsequently classified according to its level of sensitivity by using one of the recognized levels of classification:

- 6.1.2.3.1 Confidential;
- 6.1.2.3.1 Secret; and
- 6.1.2.3.2 Top Secret.

6.1.2.4 Employees of the department of Public Works, Roads and Transport who generate sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labeling of classified documents.

6.1.2.5 The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times.

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

- 6.1.2.6.1 Intrinsic secrecy approach;
- 6.1.2.6.2 Need-to-know;
- 6.1.2.6.3 Level of security clearance.

6.1.3 COMMUNICATION SECURITY

The Security Manager is responsible for the management, integration, and implementation of the system security architecture and maintenance of information and communication technology system for the Department that is in compliance with the MISS document.

6.1.4 INFORMATION TECHNOLOGY SECURITY

All computer storage media (visual, magnetic or optical) are documents in terms of the definition in the Protection of Information Act 84 of 1982 (as amended). These documents when containing classified information shall be handled in accordance with the document security standards.

6.1.5 PHYSICAL SECURITY

The physical security measures shall be implemented to:

- 6.1.5.1 Delay or prevent unauthorized access to assets and information of the Organization.

- 6.1.5.2 Detect any attempt or actual gaining of unauthorized access to such assets or information; and
- 6.1.5.3 Activate appropriate responses to such attempts or actual gaining of unauthorized access.
- 6.1.5.4 Secure storage, transportation, transmission and disposal of all classified information and other assets of the Organization.
- 6.1.5.5 The physical patrolling of government buildings
- 6.1.5.6 Timely reporting of all incidents to the security manager.
- 6.1.5.7 The following shall be adhered to as stipulated in the MISS document:
 - 6.1.5.7.1 Access Control (searching, escorting)
 - 6.1.5.7.2 Key Control;
 - 6.1.5.7.3 Office Security:
 - 6.1.5.7.4 Movement of assets (recording of information)

6.2 CONTINGENCY PLAN/BUSINESS CONTINUITY PLANNING

The contingency plan is aimed at preventing, combating any disaster and emergency. The contingency plan shall be geared for saving lives, safeguarding property and information and ensuring that activities can continue with as little disruption as possible.

6.3 SECURITY INCIDENTS/BREACHES REPORTING PROCESS

All matters of security breaches shall be noted and immediately reported to the Security Manager for investigation.

Loss of any computer and peripheral equipment, such as note-books, laptops, portable PCs shall be reported to the Security Manager, who in turn must relay the matter to the National Intelligence Agency, South African Police Service and South African Communication Security Agency in case of cryptographic equipment being also involved in the loss.

Breaches of security shall always be dealt with the highest degree of confidentiality in order to protect the official(s) consent and to avoid divulgence of sensitive information.

6.4 STAFF ACCOUNTABILITY AND ACCEPTABLE USE OF ASSETS

All Departmental assets shall be used in the interest of the Department with due care, consideration and without abuse or neglect, and as such are returned to the Department at time of termination of service.

6.5 LOSSES OR DAMAGES OF STATE /PROPERTY

The Accounting Officer or delegated official shall report all losses or damages arising from criminal acts or omissions to the Auditor General and the Provincial Treasury. All thefts of departmental assets shall be reported to the Police within 48 hours and to Security section in writing at Head Office after obtaining the case number and copy it to Asset section.

Security section shall conduct internal investigation and if it is found that the loss or damages are the negligence of the security company, the damages or losses shall be recovered from the security company or they shall be given time to replace the state assets. In case an official is liable for such loss or damage of state assets the value of such loss or damage shall be recovered from him or her.

6.6 SECURITY AWARENESS AND TRAINING

The Security Manager shall develop and implement security training and awareness programme for the Department with the assistance of:

- 6.6.1 The Security Committee and training unit of the Department
- 6.6.2 The SAPS and National Intelligence Agencies with regard to their respective fields of responsibilities and
- 6.6.3 The inter-departmental forums for Security Managers

6.7 OATH OF SECRECY

Managers shall ensure that all employees of the Department are informed of their legal obligation to refrain from divulging classified information to unauthorized parties, states, institutions or individuals. Managers shall ensure that contents, meaning and implications of the legislation relevant to the protection of information are explained to the relevant employees/persons and that they formally acknowledge that they have been notified by signing Oath of Secrecy forms on assuming and relinquishing duties in or on behalf of the Department, and in cases of amendment to the Oath of Secrecy form.

7. ROLES AND RESPONSIBILITIES

- 7.1 The head of the Department of Public Works, Roads and Transport is accountable and shall designate the Security Manager to manage the total security function of the Department.
- 7.2 The Security Manager is accountable for all security measures related to the department. She/he shall develop security policy and procedure manual and shall oversee that the implementation and execution of a Security Policy for the Department of Public Works, Roads and Transport takes place. The Security Manager shall identify and coordinate vetting for all officials and service providers who are having access to sensitive information.
- 7.3 Security Committee shall comprise of representatives of the internal security, various programmes and directorates. Their responsible is to:
 - 7.3.1 Co-ordinate and integrate all the security activities within the Department with the aim of good governance.
 - 7.3.2 Evaluate security risk and approve strategies and measures.
 - 7.3.3 Evaluate security breaches and approve rectification measures
- 7.4 Employees shall be required to act responsibly to ensure that information and assets are secured within the Department.
- 7.5 Line managers are responsible to ensure that information, people and assets are protected and to report any breaches to the Security Manager.

8. MONITORING AND EVALUATIONS

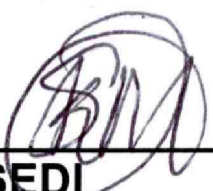
The Security Management section shall monitor the implementation of the policy and shall report any deviations to the Head of the Department. Ongoing security audits will be conducted to evaluate and measure Security compliance by conducting inspections and reporting inefficiency in the Security systems.

9. POLICY REVIEW

The review of this policy shall be done in accordance with the changing legal framework.

10. APPROVAL

Approved



K.M. MOHLASEDI
HEAD OF THE DEPARTMENT

DATE

10/10/2011