Department of Public Works, Roads and Transport

MPUMALANGA PROVINCIAL GOVERNMENT

SECURITY MANAGEMENT POLICY

Issue: 3.0

Responsible Section: ..... Security Management

Date of Approval: 13/10/2025

MPUMALANGA
THE PLACE OF THE RISING SUN

TABLE OF CONTENTS

ABBREVIATIONS

DPWRT	Department of Public Works, Roads and Transport
MEC	Member of the Executive Council
MMS	Middle Management Services
PSR	Public Service Regulation, 2016
MISS	Minimum Information Security Standards
MPSS	Minimum Physical Security Standard
SSA	State Security Agency
SM	Security Manager
SAPS	South African Police Service
SOP	Standard Operating Procedure

DEFINITIONS

Accounting Officer	Means	A person mentioned in section 36 of the Public Finance Management Act, 1999 (Act No.1 of 1999) and includes any person acting as the Accounting Officer;
Department	Means	Department of Public Works, Roads and Transport;
Confidential-Classification	Means	Is the classification given to information that may be used by malicious/opposing/hostile elements to harm the objectives and functions of an individual and/or institution.
Secret- Classification	Means	Given information that may be used by hostile/opposing/malicious elements to disrupt the objectives and functions of officials or and Department;
Top Secret-Classification	Means	Given information that can be used by enemies or hostile/malicious elements to neutralize the objectives and functions of the Department.
Security Principles	Means	Foundation upon which security policies can be further developed;
State Property	Means	Immovable and movable assets of the Department of Public Works, Roads and Transport; and

1. INTRODUCTION

The Department is striving to provide safety and secure its assets against the potential threats internal, external, man made and natural, which may have negative effect on the Department's effectiveness to deliver services, should these threats are not controlled/managed properly.

2. OBJECTIVES

The objective is to:

Support the national interest and the Department business objectives by protecting employees, information and assets thereby assuring continued delivery of services to South African Citizens.

3. REGULATORY FRAMEWORK

The following legislations guides this policy:

3.1. Control of Access to Public Premises and Vehicles Act, 1985 (Act No. 53 of 1985);

3.2. Criminal Procedure Act, 1977 (Act No. 51 of 1977);

3.3. Firearms Control Act, 2000 (Act No. 60 of 2000);

3.4. Minimum Information Security Standard (MISS);

3.5. Minimum Physical Security Standard;

3.6. Departmental loss Control Policy;

3.7. Private Security Industry Regulatory Authority Act, 2001 (Act No. 56 of 2001);

3.8. Protection of Information Act, 1982 (Act No. 84 of 1982); and

3.9. Trespass Act, 1959 (Act No. 6 of 1959).

3.10 Occupational Health and Safety Act, 1993 (Act No. 85 of 1993);

3.11 Records Management Policy and the Provincial Archives Act, 1998 (Act No. 14 of 1998)

4. SCOPE OF APPLICATION

This policy shall be applicable to all employees, contractors, consultants and anyone who enters the premises managed by the Department.

5. POLICY STATEMENT

5.1 Categories of Security

5.1.1. Personnel Security

5.1.1.1 Security Screening

All employees, contractors and consultants of the Department who requires access to classified information and critical assets in order to perform their duties or functions, shall be subjected to a security screening investigation conducted by the State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

a) 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;

b) A security clearance provides access to classified information subject to the need-to-know principle;

c) 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 services with the Department; and

d) 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 of a more frequent basis as determined by the Accounting Officer, based on information which impact negatively on an individual's security competence.

5.1.2 Document Security

The Department must ensure that every document in its possession and control which falls under one of the categories of information (Top Secret, Secret and Confidential), is properly classified in accordance with the relevant level of classification as set out in the Minimum Information Security Standards (MISS) document. Disposal of records shall comply with the Records Management Policy and the Provincial Archives Act, 1998 (Act No.14 of 1998).

5.1.2.1 Categorization of Information and Information Classification System

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

5.1.2.2 Sensitive Information

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

a) State Secret;
b) Trade Secret; and
c) Personal Information.

5.1.2.3 Levels of Classification

a) The categories must further be classified according to the level of sensitivity by using one of the recognized levels of classification:
    i. Confidential;
    ii. Secret; and
    iii. Top Secret.
b) Employees of the Department who generate sensitive information are responsible for determining information classification levels and the categories thereof, subject to management review. This responsibility includes the labeling of classified documents.

c) 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.

5.1.2.4 **Access to Classified Information shall be Determined by the Following Principles**:

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

5.1.3 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 and ensure compliance with the MISS document.

5.1.4 Information Technology Security

All computer storage media (visual, magnetic or optical) are documents in terms of 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 as prescribed in the MISS and departmental IT policy.

5.1.5 Physical Security

The physical security measures must be implemented to:

a) Delay or prevent unauthorized access to assets and information of the Organization;
b) Detect any attempt or actual gaining of unauthorized access to such assets or information;
c) Activate appropriate responses to such attempts or actual gaining of unauthorized access;
d) Secure storage, transportation, transmission and disposal of all classified information and other assets of the Department;

e) Physically patrol the government buildings;

f) Timely report all incidents to the Security Manager; and

g) Adherence to stipulations of MISS document in terms of the following:

I. Control of Access to Public Premises and Vehicle Act, 1985 (Act No. 53 of 1985) which include all principles of access control. These principles are further explained in details in the Standard Operating Procedure (SOP) for PWRT.

II. Key Control;

III. Office Security and

IV. Movement of assets (recording of information).

5.2 Contingency Plan/Business Continuity Planning

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

5.3 Security Incidents/Breaches Reporting Process

5.3.1. All matters of security breaches must immediately be reported to the Security Manager.

5.3.2. The matter must be investigated by the relevant authority.

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

5.3.4. Computers and Laptops

5.3.4.1 Use of laptops and computers by employees must be restricted to official purpose only.

5.3.4.2 Users to be made aware of the terms and conditions and responsibility for safekeeping of the asset and the security of information held on the device.

5.3.4.3 Loss of any computer and peripheral equipment, such as note-books, laptops, portable PCs must be reported to the Security Manager, who in turn

must relay the matter to the State Security Agency, South African Police Service and South African Communication Security Agency or any relevant authority in case of cryptographic equipment being also involved in the loss. Read with Departmental IT Policy

5.4 Staff Accountability and Acceptable Use of Assets

All Departmental assets must be used in the interest of the Department with due care, consideration and without abuse or neglect, and must be returned to the Department at time of termination of service and at the end of the asset life span. Refer to the IT Security Policy and Asset Management Policy.

5.5 Losses or Damages of State Assets

5.5.1 All cases of theft, losses and damages must be reported to the nearest South African Police Service within forty-eight (48) hours, by the owner of the asset or the official who the asset is under the area of his/ her responsibility A full report with the case number and the serial number of the asset, if any must be submitted to the Responsibility Manager, Security Management/ Loss Control Officer and Asset Management irrespective of the monetary value of the loss or damage. Officials at District Offices shall report to the relevant district Security Manager. The Loss Control Officer must conduct internal investigation and prepare a report with findings and recommendations and submitted to the Accounting Officer.

5.5.2. In cases where the official concerned cannot report the incident within 48 hours due to injuries sustained during the incident, the Responsibility Manager must report to Security Management and Asset Management in writing within 48 hours.

5.5.3 If the official is found to be liable of such loss or damage of the state asset due to negligence, the matter must be referred to Labour Relations for consequence management.

5.6 **Security Awareness and Training**

The Security Manager must develop and implement security training and awareness programme for the Department.

5.7 **Oath of Secrecy**

All employees must sign the oath of secrecy which inform them of their legal obligation to refrain from divulging classified information to unauthorized parties.

6. ROLES AND RESPONSIBILITIES

6.1 The Accounting Officer shall:

a) Be responsible for the effective and efficient implementation of this policy as part of internal control within the Department.

b) Designate the Security Manager to manage all aspect of Security the total security function of the Department;

6.2 The Security Manager shall:

a) Identify and coordinate vetting for all officials and service providers who are having access to sensitive information; and

6.3 **The Security Committee** shall comprise of representatives of the internal security and relevant programs and directorates, and shall be responsible to:

6.3.1. Co-ordinate and integrate all the security activities within the Department with the aim of good governance;

6.3.2. Evaluate security risk and approve strategies and measures;

6.3.3. Evaluate security breaches and approve rectification measures;

6.3.4. Develop security policy and make recommendations as per the advice from SSA and SAPS;

6.3.5. Make recommendations to the Accounting Officer regarding the implementation and maintenance of security measures;

6.3.6. Review security policy jointly with the SAPS and SSA or as and when the need arises;

6.3.7. To conduct awareness and promote Security Management Policy to staff and stakeholders;

6.3.8. Administer reports on theft and losses and make recommendations to the Labour Relations section as well as to the Accounting Officer in a bid to minimize future losses.

6.4 Employees have a responsibility in ensuring that personnel, information and assets are secured within the Department; and

6.5 Line managers are responsible to ensure that information, people and assets are protected and to report any breaches to the Security Manager.

7. MONITORING AND EVALUATION

The Security Management Section shall monitor and evaluate the implementation of this policy.

8. POLICY REVIEW

The policy shall be reviewed every 3 years or as and when there is a need to factor in changes in legal framework as well as economic trends.

9. DEVIATIONS

Any deviation from this policy shall be subject to the approval of the Accounting Officer.

10. IMPLEMENTATION DATE

The policy shall come into effect from the date of approval by the Accounting Officer.

11. APPROVAL

MR MC MOROLO
HEAD: PUBLIC WORKS, ROADS AND TRANSPORT
DATE 13 | 10 | 2025.