LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
PUBLIC WORKS, ROADS & INFRASTRUCTURE

Policy Name	**Integrated Security Policy**
The revision / version of the policy	**02**
Domain	**Security Risk Management**

TABLE OF CONTENTS

1. ACRONYMS AND ABBREVITIONS

SSA : State Security Agency
SANDF : South African National Defence Force
SAPS : South African Police Service
SASS : South African Secret Service
MISS : Minimum Information Security Standards
MPSS : Minimum Physical Security Standards
LDPWRI : Limpopo Department of Public Works, Roads &Infrastructure

2. INTRODUCTION

The Department of Public Works, Roads & Infrastructure (LDWRI) fully accepts its responsibilities to, as far as practically possible; ensure a safe and secure environment for its employees, clients, contractors and visitors, as well as to safeguard all public assets and information entrusted to it.

In terms of the provisions of Chapter 3.6 of the Minimum Physical Security Standards, 2009, the Head of the Department is accountable for the overall physical security under his/her control. The Head of the Department must also oversee the development, implementation and maintenance of the security policy as per the needs of the Department.

The Constitution of the Republic of South Africa (bill of rights), specify that the security division has the mandate and responsibility to execute various parts of legislation that could constitute an infringement of individual rights.

Without derogating from the above, the Department also acknowledges the limitations of scarce public resources and, therefore, the need to strike a workable balance between effective security measures and its obligation to provide efficient public services to the citizens of the Limpopo Provincial Government.

In the application of its security policy, the Department of Public Works will diligently follow the principle of minimum force. The professionalism required for dealing with the safeguarding of Government properties will be supported by well-designed and comprehensive awareness programmes, capacity building programmes, as well as building partnership with other stakeholders.

3. PURPOSE AND OBJECTIVES

3.1 The purpose

3.1.1 To lay down a set of security rules by which all employees of the Department of Public Works and all its stakeholders must abide by.

3.1.2 Guide people's conduct while providing a base-line to procure, implement and evaluate security systems.

3.2 The Objectives

3.2.1 Managing the security risk problem into a workable solution.

3.2.2 Managing security and risk awareness towards sound mitigation applications.

3.2.3 Maintenance of a safe and secure workplace.

3.2.4 Protection of departmental assets and information.

4. AUTHORITY OF THE POLICY

This policy is authorized and issued by the Member of Executive Council for Limpopo Provincial Department of Public Works, Roads and Infrastructure.

5. LEGAL FRAMEWORK/ MANDATES

a. RSA Constitution,1996 (Act No 108 of 1996)
b. Minimum Physical Security Standards (MPSS)
c. Minimum Information Security Standards (MISS)
d. Control of Access to Public premises and Vehicles Act, 1985 (Act No 53 of 1985)
e. Criminal Procedure Act, 1977 (Act No 51 of 1977)
f. National Strategic Intelligence Act, 1994 (Act 39 of 1994)
g. Disaster Management Act, 2002 (Act No 57 of 2002)
h. Firearm Control Act, 2000 (Act No 60 of 2000)
i. Hazardous Substances Act, 1973 (Act No 15 of 1973)
j. Intimidation Act, 1982 (Act No 72 of 1982)
k. National Building Regulations and Building Standards Act,1977 (Act No103 of 1977)
l. National Archives of South Africa Act, 1996 (Act No 43 of 1996)
m. Occupational Health and Safety Act, 1993 (Act No 85 of 1993)

n. Private Security Industry Regulation Act, 2001 (Act No 56 of 2001)
o. Promotion of Access to Information Act, 2000 (Act No 2 of 2000)
p. Protection of Information Act, 1982 (Act No 84 of 1982)
q. Protection of Personal Information Act, 2013 (Act No 4 of 2013)
r. Protected Disclosure Act, 2000 (Act No 26 of 2000)
s. Public Service Act and Regulations,2001
t. Regulations and Provincial Treasury Directives
u. Public Finance Management Act, 1999 (Act No 1 of 1999)

6. SCOPE OF APPLICATION

This policy is applicable to all employees, stakeholders both internal and external as well as Visitors and Contractors. This policy is applicable to all facilities or administrative areas, owned or controlled by the Department of Public Works, Roads & Infrastructure.

7. DEFINITION OF TERMS

Access Control	The process by which access to a particular area is controlled or restricted to authorised personnel only.
After Hours	a) The time between 16H30 – 07H00 b) Saturdays and Sundays; and c) Public Holidays.
Classification	The grading/arrangement or re-grading/re-arrangement of a document, in accordance with its sensitivity or in compliance with a security requirement. All official matters requiring the application of security measures (exempted from disclosure) must be classified:
Confidential	relates to all information that may be used by malicious/opposing/hostile elements to harm the objectives and functions of an individual or Department.
Secret	relates to all information that may be used by malicious/opposing/hostile elements to disrupt the objectives and functions of the department and or state.
Top Secret	relates to all information that may be used by malicious/opposing/hostile elements to neutralise the objectives and functions of the Department and or State.
Contingency	refers to the prior planning of any action that has the purpose to prevent,

Planning	and or combat, or counteract the effect and results of an emergency where lives, property or information are threatened. This includes compiling, approving and distributing a formal written plan and the practice therefore, in order to identify and rectify gaps in the plan, and to familiarise personnel and co-ordinators with the plan.
Compromise	Compromise refers to the unauthorised disclosure/exposure or loss of sensitive/classified information, or exposure of sensitive operations, people or place, whether by design or through negligence.
Declaration of Secrecy	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.
Destruction of classified material	Expunging or destroying of classified/sensitive documents.
Document	In terms of the provisions of the Protection of Information Act, 1982 [PIA] (Act, 84 of 1982), a document is any note or writing, whether produced by hand or by printing, typewriting or any other similar process, any copy, plan, sketch or photographic or other representation of any place or article or any disc, tape, card, perforated roll or other device, in, or on which sound or any signal has been recorded for reproduction.
Document Security	The conscious provision and application of security measures in order to protect classified/sensitive documents.
Espionage	The methods by which states, organisations and individual, attempt to obtain classified information to which they are not entitled.
Information Security	That condition created by the conscious provision and application of a system of document, personnel, physical, computer and communication security measures to protect sensitive, classified and valuable information.
Need to know principle	The furnishing of only that classified information or part thereof that will enable a person/s to carry out his/her task.
Personnel Security	Personnel security is that condition created by the conscious provision and application of security measure in order to ensure that any person who gains access to sensitive/classified information has the necessary security clearance, and conducts himself/herself in a manner not exposing him/her or the information to compromise. This could include mechanisms to effectively manage and solve personnel grievances, etc.
Physical Security	That condition which is created by the conscious provision and application of physical security measures for the protection of personnel, property, assets and information.

Premises	For the purpose of this policy, premises shall refer to any building, structure, hall, room, office, land, enclosure or water surface which is the property of, or is occupied by, or is under the control of the Department of Public Works and to which a member of the public has a right of access.
Screening Institution	Screening institutions are those institutions (the SAPS, SSA, SASS, and 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 conduct security clearance employees within the Public Service.
Security	Security is concerned with the provision and application of appropriate standards and measures intended to provide protection to people, property, information and other assets against the security risks and most threats to which they are exposed.
Security area	Any area to which the general public, and in some cases, certain employees are not freely admitted and to which only authorised persons are admitted.
Security audit	That part of security control undertaken to determine the general standard of information security and to make recommendations where shortcomings are identified, evaluate the effectiveness and application of security policy/standards/procedures and to make recommendations for improvement where necessary; provide expert advice with regard to security problems experienced; and encourage a high standard of security awareness.
Security clearance	Security clearance refers to an official document that indicates the degree of security competence of a person.
Security competence	This is a person's ability to act in a manner that he does not cause classified information or material to fall into unauthorised hands, thereby harming or endangering the security or interests of the State/Department. Security competence is normally measured against the following criteria: susceptibility to extortion or blackmail, amenability to bribes and susceptibility to being compromised due to compromising behaviour, and loyalty to the State/Department.
Security Screening	It is the systematic process of investigation undertaken to establish the security competence of an employee with the intention of protecting the State and its inhabitants from foreign intelligence services and corruption.
Sensitive/Classified information	Information, which in the national interest is held by, produced in, or is under the control of the Department, or which concerns the department and must, by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.
Storage	The safekeeping of classified documents in appropriate (Prescribed) lockable containers, strong rooms, record rooms and reinforced rooms and safes.
Transmission security	Transmission security is a part of communication security and entails the safeguarding and secure use of systems linked to one another for the sake of communication.
Visitors	Non-employees or members of the public

8. POLICY PRONOUNCEMENT

This policy provides the management of the following security related matters: -

a. **Physical Security**, i.e. physical measures aimed at the protection of personnel, property, assets and information.
b. **Personnel Security**, i.e. measures aimed at ensuring that any person who gains access to classified information has the necessary authority and security clearance to do so.
c. **Document Security**, i.e. measures aimed at protecting classified and sensitive documents.
d. **Information Security**, measures aimed at protecting sensitive, classified and valuable information.
e. **Communication Security**, i.e. measures aimed at protecting classified and sensitive information that needs to be communicated.
f. **Information Technology Security**, i.e. measures aimed at ensuring the confidentiality and integrity of data, as well as the availability of data and systems.

8.1 Division of Roles and Responsibilities

8.1.1 Head of Department: Department of Public Works

8.1.1.1 In terms of the provisions of Chapter 3.6 of the Minimum Physical Security Standards, 2009, the Head of the Department is accountable for the overall physical security under his/her control. The Head of the Department must also oversee the development, implementation and maintenance of the security policy as per the needs of the Department.

8.1.1.2 He/she must ensure that the Security Manager is appointed to manage all security functions and ensure implementation/adherence to security standards.

8.1.1.3 He/she must ensure that employees and service providers [contractors, consultants] are subjected to reliability record checking process conducted by SSA.

8.1.1.4 The Head of the Department must also ensure that training and awareness programmes with regard to adherence to the minimum security standards are conducted.

8.1.1.5 The Head of the Department must also ensure that the Security Committee is established within his/her Department.

8.1.1.6 He/she must see to it that a correct reporting structure is in place with regarding to reporting of security breaches.

8.1.1.7 The Head of the Department must approve budget as advised by the Security Committee for the recommendations on the security assessment conducted SAPS and Security Component in the Department.

8.1.1.8 With the assistance of the Security Committee, the Head of the Department must also ensure that there is continuous monitoring of the compliance with the minimum security standards by instituting internal Departmental Policy or directives.

8.2 Responsibilities of Security Manager

8.2.1 In terms of the provisions of Chapter 3.7 of the Minimum Physical Security Standards, 2009, must manage all matters relating to the administration and organisation of security at the Department.

8.2.2 He/she must draft security policy for approval by the Security Committee and Head of the Department

8.2.3 He/she must manage the Security Component of the Department.

8.2.4 The Security Manager must continually monitor all physical security related contracts at the Department to ensure compliance with the contract specifications.

8.2.5 He/she must ensure that security assessments/evaluations/threats and risk assessments of the installations are conducted by SAPS and Departmental Security Personnel.

8.2.6 He/she must enhance the awareness of the staff regarding physical security in the Department.

8.2.7 The Security Manager must analyse the audit results, make recommendations to the Head of the Department to improve physical security measures and prepare a

report for the Head of the Department for submission to SAPS regarding the findings.

8.2.8 He/she must consult with SAPS on any new developments or changes in the physical security environment.

8.2.9 He/she must ensure that applications for criminal record checks are correctly completed before submission to SAPS.

8.2.10 The Security Manager must act as chairperson of the Security Committee of the Department.

8.3. Functions of the Security Committee

8.3.1. The Security Committee shall be established and comprised of representatives from all the Programmes to carry out the following functions: -

8.3.1.1. Recommend the security policy of the Department after having taken the advice provided by SAPS and SSA into account.

8.3.1.2. Make recommendations to the Head of Department regarding the implementation and maintenance of security measures.

8.3.1.3. Regularly reviews the security policy of the Department, its prioritisation thereof as well as information and advice provided by SAPS and SSA.

8.3.1.4. Forward the draft policy and any review thereof to SAPS and SSA for indorsement, then ensure approval by HOD.

8.3.1.5. Ensure the communication of the approved policy to all staff members and relevant consultants and contractors.

8.3.1.6. Make recommendations to the Head of Department regarding directives to be issued by the Head of the Department to ensure the implementation of the security policy and any review thereof.

8.4. Responsibilities of Security Management Component

8.4.1 The Security Management Component is responsible for the control and co-ordination of all security matters in the Department.

8.4.2. It must ensure that policies, procedures and standards are maintained throughout the Department and must promote dissemination of instructions and efficient reporting of incidents to the relevant Programme managers and government agencies.

8.4.3 To oversee performance of private security in terms of Service Level Agreement.

8.5. Responsibilities of Employees

8.5.1 Effective security measures requires a careful thought, co-operation and concerns from all employees, the support of all employees is indispensable to control security breaches and losses at the workplace. Therefore, all employees of the Department are expected to make their contributions by:

I. Locking away valuable assets and sensitive documents in cabinets when not in use;
II. Securing their workstations/office layout and restricting access/entrance (office security);
III. Disposing of classified/sensitive papers in an appropriate manner (shredding);
IV. Not storing or saving sensitive/classified information on laptops;
V. Reporting suspicious visitors to security breaches (e.g. theft); and
VI. Reporting suspected security breaches (e.g. theft); and
VII. Looking after their keys and ensuing that such keys do not fall into the wrong hands.

8.5.2. Frequent efforts shall, therefore, be made to raise the awareness level amongst the officials on the importance of security and the strict execution of the security procedure.

8.5.3. Senior Managers are responsible for the implementation of all security measures within their components. This applies to all Provincial Government Buildings.

8.6. SAPS: VIP Protection and Security Services Unit

8.6.1 SAPS VIP Protection and Security Unit is an integral part of the government's overall security infrastructure. This Unit is responsible for all security arrangements regarding the Provincial Legislature, as well as the Members of the Executive Council.

9. PHYSICAL SECURITY MEASURES

9.1 Security Appraisals

9.1.1 The Departmental Security Manager, after consultation with the designated structures of the SSA and SAPS, must at least on a quarterly basis present a strategic security appraisal to the Head of Department and the Security Committee.

9.1.2. This appraisal must address the Department's vulnerabilities/risks/threats in respect of Physical-Personnel- Document- Communication and Information Technology Security). An assessment/evaluation of current security policies and practical measures against real and potential threats must be included in such appraisals, together with proposals to deal with contingencies in this regard.

9.2. Security Audits

9.2.1 In addition to the security audits that the **SSA/SAPS** will initiate on own accord in pursuance of its statutory mandate, the Head of Department may request SSA or Security Management Personnel to conduct security audits in his/her Department, or specific components thereof, to determine compliance with security policies and the state of preparedness.

9.3. Access Control/Egress Control

9.3.1. The purpose of access control is to safeguard public premises and vehicles and to protect personnel and information therein. Access control includes both electronic and physical searches aimed or directed to theft prevention.

9.3.2. The Head of Department must institute measures in conjunction with the Security Manager to control access and movement in premises under their control by employees, visitors and service providers.

9.3.3 Access control measures must be of such a nature as to ensure that any person wanting to gain access to a departmental premise is safe, has a valid reason to enter, is entitled and authorised thereto, and that the department or its employees will not be exposed to any danger or to breaches of security.

9..3.4 Access control must be dealt with in terms of the provisions of the Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985). This Act empowers the Head of Department to, among others, take such steps as he/she consider necessary to safeguard public premises and protect people thereon against dangerous objects.

9.3.5 The Security Manager must ensure that appropriate notices are displayed at all public entrances to department premises to the effect that access to the premises is subjected to the provisions of the Control of Access to Public Premises and Vehicles Act, 1985.

9.3.6 The Head of Department may in writing determine different levels or degree of access control to different public premises (or parts thereof) under their control, including restricted access by employees to their offices after normal office hours.

9.3.7. In those instances where persons are required to identify themselves before access to the premises is authorised, only the following are deemed to be positive identification:-

a. RSA bar-coded identity document/ Smart ID card.
b. Valid RSA passport.
c. Valid RSA driver's licence.
d. Access Cards for employees of the Department to verify identification.
e. Valid access permit issued by a person who is duly authorised by the Head of Department of Public Works (employees, consultants and contractors).
f. Identification Cards from SAPS, SANDF and SSA.

9.3.8 All access permits issued must be returned to the issuing authority at the termination of their service. The issuing authority must dispose of such permits appropriately.

9.3.9 All persons entering the premises of the Department of Public Works must display their access cards/permits conspicuously at all times.

9.3.10 All vehicles (private or government owned) must be searched when entering and leaving the premises of the Department. Property, equipment, parcels, documents, etc. will only be taken out of the buildings with official removal permits signed by an authorised official.

9.3.11. In terms of section 2(2) of the Access to Public Premises and Vehicle Act, 1985 Head of the Department may require that an authorised officer search any person and/or vehicle for dangerous objects at all access control points. Random searches may be conducted after hours or at any other time.

9.3.12. Emergency exits should only be used when there is a security emergency and Investigation will be done for any unnecessary use of the escape doors.

9.4. Escorting

9.4.1 All visitors must report at reception of the Department's buildings for security to confirm such visits.

9.4.2 When necessary, security guards have to escort visitors to their destinations. Alternatively, visitors must remain at the reception area for collection by the host, and must therefore be returned by the particular host.

9.5. Key Control and Combination Locks

9.5.1 The Security Manager must ensure effective control of keys and records of keys, including duplicate keys, to buildings/premises as well as to safes and strong rooms.

9.5.2 The Security Manager must ensure that a key custodian is appointed in writing.

9.5.3 Loss of keys must immediately be reported to the key custodian.

9.5.4 Lost keys shall be replaced with applicable costs as determined by the revenue management including lock replacement at a price relevant at the time.

9.5.5 The keys to any building, part of a building, room, strong room, safe, cabinet or any other place where classified material is kept must be locked away after which utmost care and effective key control must be instituted.

9.5.6 The keeping of the necessary key registers, control and safe of duplicates keys must be strictly adhered to.

9.5.7 If a strong room or safe is fitted with a combination lock, the combination must, apart from being reset when it is purchased, be changed at least once every three months, or on the following occasions:

a) When it is suspected that it has been compromised or tampered with.
b) On resumption of duty by the responsible officer after a continuous period of absence, whether on vacation leave or for official reasons,
c) if the combination had necessarily to be made known to some other person for use during the period concerned.
a. When a new user takes over.

9.5.8 The inspection of the contents of such safe or strong-room must be done in the presence of any such person who had been in control such container, be a safe or strong room.

9.5.9 When a combination is reset, the following rules must be adhered to with: -

a) The figures making up a specific combination should not be used more than once in succession, even if they are in a difference order.
b) Avoid the use of members with some personal significance, e.g. Age, date of birth, telephone numbers, street addresses and numbers of safes, etc. Also avoid the figures zero (0), five (5), ten (10) and multiples of the last two. High and low numbers should preferable be used alternately (e.g. 68-13-57-11).
c) Only the users may set a combination lock.
d) Knowledge of a combination should be restricted to the minimum number of person's desirable on the grounds of operational requirements, e.g. in the case of a communal safe.

9.5.10 After the combination has been reset, the new combination must be handed to The key custodian or another person designated for the purpose, in a sealed envelope for safe custody, so that he can complete the combination lock register.

9.5.11 As far as safe and strong room keys and the combinations of cryptographic Centres are concerned, the requirements contained in the Communication Security Instructions must be complied with.

9.6. Maintenance Services, Repairs, and the Cleaning of Buildings/Offices

9.6.1 Occupants of offices where classified or sensitive matters are dealt with, must always be present when artisans, technicians or cleaners are performing their duties. Special care should be taken on such occasions to ensure that they do not gain access to classified matters.

9.7. Office Security

9.7.1 It is the responsibility of every employee to identify and enquire or assist strangers who are roaming about in the building or offices.

9.7.2 Under no circumstances must a visitor be left alone in an office where classified information is dealt with.

9.7.3 Contractor services must be performed during working hours for the prevention of security breaches that might take place after hours. If such a service must be performed after hours, arrangements must be made with Security Management Component for monitoring and supervision.

9.7.4 Offices must be locked at all times when the occupant goes out, even on short periods and electrical appliances must be switched off.

9.7.5 Personal items such, as handbags, briefcases, wallets, cellphones, etc. must not be left unattended at open spaces, on the tables and even drawers, since they could be stolen.

9.7.6 Keys must not be left hanging on the door locks, padlocks, lockable facilities and padlocks/locks to lockable facilities must be locked at all times.

9.7.7 Office windows must be closed when the office is unattended and lights must be switched off after hours to conserve energy.

9.8. Procurement of Private Security Services

9.8.1 Private security services, be it longer term or emergency, will be procured in terms of current statutory and other applicable prescripts. e.g. Supply Chain Management Policy.

9.8.2 To protect the department's legal and operational interests, the Department would, as a general guideline from a security point of view, prefer to outsource security

services to service providers in respect of whom it has been verified by the departmental security managers that they comply with the following conditions: -

a. Registration with Security Regulatory Authority in terms of the applicable legislation.
b. Registration with the relevant authority in terms of the applicable trade legislation (e.g. Companies Act]
c. Registration with the relevant authorities in terms of the Compensation for Occupational Injuries and Diseases Act, 1993 (Act No. 130 of 1993) and the Unemployment Insurance Fund.
d. Registration in terms of the relevant tax legislation (e.g. income tax and VAT).
e. Accepted full responsibility in terms of section 37(2) of the Occupational Health and Safety Act, 1993 (Act No.85 of 1993).
f. Is in good standing with Security Regulating Authorities, South African Revenue Services and other authorities indicated above.
g. Subject to security clearance issued by State Intelligence Agency of the service provider as well as staff members.
h. Has a work force that is: –
    - Duly registered with the Private Industry Security Regulatory Authority and properly trained in terms of the Authority's requirements; and
    - Administered and managed in terms of the relevant labour laws, including the Employment Equity Act, 1998 (Act No.55 of 1998), Labour Relations Act, 1995 (Act No.66 of 1995) and Basic Conditions of Employment Act, 1997[Act No. 75 of 1997], Minimum Wage Act, etc.
i. Has the operational capacity to properly control and support all operational staff, including adequate control room facilities, communications infrastructure, transport and contingency capacity.
j. Is in financial good standing to reasonably cover any liabilities incurred due to the unlawful acts, omissions and/or negligence by staff in rendering services to the Department, with the understanding that public liability insurance commensurate with the potential risks to which the service provider are exposed to , will suffice.

9.8.3 Contractual arrangements between the Department and the preferred service provider should, apart from the general stipulations, as a minimum include the following provisions:

a. Liabilities of the service provider, including liability for any loss or damage to property due to, among others, the negligence or omissions of the service provider's personnel, or to their non-performance of contractual service obligations.

b. Conditions for the summarily termination or suspension of the service providers' by the Department. In this regard the service provider's inability to comply with the requirements in the above paragraph, as well as the inability to render the level and quality of operational services as contracted in terms of the site and post specifications, should feature prominently.

c. Prohibition of the use of sub-contractors by the service provider. Cession agreements may be entered into in terms of the provisions of paragraph 28 of the Conditions of the Bid

d. Conditions upon which the Department can insist that a particular member of staff of the service provider be summary removed from its premises, failure to reasonable comply with minimum security instructions as set out in above paragraph, and standing operating procedures should feature prominently in this regard.

e. Obligation on the service provider to report any security breaches to the Department as a matter of urgency through the prescribed channels of communication.

f. Formal channels of responsibility within and communication between the Department and the service provider.

9.8.4 All service providers who bids for security services should be informed beforehand of the risk assessment and general conditions (paragraph above) as well as the procurement provisions applicable, preferably as part of the prescribed Bidder documentation to be supplied to potential bidders.

9.9. Monitoring of Compliance with Service Level Agreement.

9.9.1 To ensure value for money it is imperative that the actual service delivery of private service providers is thoroughly monitored and controlled in terms of the contractual arrangements [SLA]. Where contractual obligations are not met, relevant remedial actions must be instituted against the service providers as a matter of urgency.

9.10. Contingency Plan

9.10.1 The Head of Department must ensure that proper contingency planning is effected for all public premises under his/her control. Contingency planning in this regard refers to prior planning to prevent, combat and/or counteract the effect of an emergency situation where lives, property or information are threatened. This includes compiling, approving, and distributing a formal written security plan, and the practise thereof to identify and rectify gaps in and to familiarise employees with the plan.

9.10.2 In compiling contingency security plans and measures (such as emergency evacuations, fire preventions and control, first aid and training emergency personnel) cognisance must be taken of the relevant provisions of the MISS, MPSS and of the statutory requirements contained in, among others, the following laws;

a. National and Local Government Disaster Management/By-laws relating to Community Fire Safety.
b. Hazardous Substances Act, 1973 (Act No15 of 1973)
c. National Building Regulations and Billing Standards Act, 1977 (Act No103 of 1977).
d. Occupational Health and Safety Act, 1993 (Act No 85 0f 1993)

10. PERSONNEL SECURITY

10.1 Overall Responsibility

10.1.1 The Head of Department assume overall responsibility to ensure that his/her personnel are vetted in terms of the relevant provisions of the MISS and this policy, including determining the various levels of security clearance for the various personnel or categories of his/her department.

10.2 GENERAL PRINCIPLES: VETTING

10.2.1 Chapter 5 of the MISS provides the following general principles/guidelines that apply in respect of security vetting:

a. Security vetting is the systematic process of investigation followed in determining a member of staff's security competence.

b. The degree of security clearance given to a member of staff security is determined by the content of and/or access to classified information entailed by the post already occupied/to be occupied.

c. Aspects such as gender, religion, race and political affiliation do not serve as criteria in the consideration of a security clearance, but actions and aspects adversely affecting the member of staff's vulnerability to blackmail or bribery or subversion and his loyalty to the State of institution does. This also includes compromising behaviour.

d. A clearance issued is merely an indication of how the member of staff can be utilised, and does not confer any rights on such a person.

e. A declaration of secrecy should be made on an official form by an applicant to any government post before he/she is appointed or during the appointment process.

f. Political office bears may not be vetted.

g. A security clearance gives access to classified information in accordance with the level security clearance, subject to the need-to-know principle.

10.3 Security Clearance: New Appointees

10.3.1 In those instances where the vetting authority is not able to issue a security clearance before the expiry of the probationary period, the letter of permanent appointment must indicate that the appointment is subject to a positive security clearance as required.

10.3.2 The limitations placed on the issuing of security clearances to immigrants, persons with dual citizenship, and persons who have lived/worked abroad for long periods as set out in Chapter 5, paragraph 3 and 4 of the MISS must be noted and adhered to.

10.4 Security Clearance for Serving Officials

10.4.1 In the case of serving official in respect of whom the vetting authority has issued a negative recommendation the Director General for SSA may be approached. A written request must be submitted to the Director General for SSA, who will after consideration make a ruling/take a decision.

10.4.2 Should the Director General of SSA not be prepared to grant approval for the issuing of clearance of those serving officials in respect of whom the vetting

authority has issued a negative recommendation, such officials should be dealt with appropriately in terms of the relevant provisions of the Public Service Act, 1994, Labour Relations Act, 1995 (Act No.66 of 1995) and applicable collective agreements.

10.4.3 As far as the transfer of officials are concerned, the Head of the receiving Department must indicate whether the official's existing security clearance is acceptable, or whether a new clearance should be requested.

10.4.4 Officials, who refuse to be subjected to security vetting and/or refuse to sign the prescribed declaration of secrecy, must be dealt with in a manner similar to that indicated in paragraph 10.4.2 above.

10.5 Vetting of Contractors and Service Providers to the Department.

10.5.1 The Head of Department must determine the security risks involved with the appointment of private contractors, including the need for and level of security clearances required.

10.5.2 Where specific security requirement has to be met by the contractor, these requirements must be contractually agreed to before commencement of service (refer to Chapter 5, paragraph 5 of the MISS).

10.6 Period of Validity of Security Clearances

10.6.1 The following levels of security clearance are valid for the period as indicated: -

a. Top Secret : 5 years
b. Secret : 5 years
c. Confidential : 10 years

10.6.2 The above mentioned requirement does not preclude re-screening at shorter intervals if so required.

10.7 Records in Respect of Security Clearances

10.7.1 The Security manager must keep records of the following: -

a. All security clearances issued by the screening authority, including contractors and temporary personnel.
b. All serving officials in respect of whom the screening authority has made a negative recommendation.

c. Original security clearance certificates shall be filed by the security management vetting unit and Personnel records, officials will only be issued with a letter indicating the status and level of their security clearance issued by SSA.
d. SSA can withdraw security clearance certificates if there are compelling security reasons.

10.8 Broad Procedure for Requesting Security Clearances

10.8.1 New appointees: Requests must be submitted to the Security Manager by the HRM Personnel Officer(s) who deal with the appointments.

10.8.2 Serving officials: Security Manager to advise supervisors of lapse of security clearances at least six months before the validity period expires.

10.8.3 Contractors: The responsible Programme Managers must submit requests to the Security Manager who will provide the necessary documentation to be completed by the individuals concerned, and arrange for the taking of the required fingerprints.

10.8.4 The completed documentation and fingerprints will be submitted to the screening authority by the Security Manager.

10.8.5 The security clearance recommendation of the vetting authority will then be submitted by the Security Manager to the Head of Department (or his delegate) for final acceptance.

10.9. Screening Authority

10.9.1 The SSA is the screening authority in terms of this policy.

11. DOCUMENT SECURITY

11.1 Classification and Reclassification of Documents

11.1.1 The Department of Public Works is in possession of information that is to some extent sensitive in nature and this obviously requires security measures. The degree of sensitivity will determine the level of protection needed to safeguard this information. This implies that the information needs to be graded or classified according to the sensitivity thereof and every classification necessitates certain

security measures with respect to the protection of such sensitive information, which such classification is known as the Grading of the document.

11.1.2 Should the author of a document on which there is no embargo, reconsider the classification of such document, he/she must inform all addressees of the new classification.

11.1.3 The receiver of a classified document, who is of the opinion that the document concerned must be reclassified, must obtain oral or written authorisation from the author, the Head of Component/ Institution or her/his delegates. Such authorisation must be indicated on the relevant document when it is reclassified.

11.1.4 When a document is classified, the classification assigned to it must be indicated clearly on the document in the following way:

11.2. Documents and bound volumes

11.2.1. The classification of loose and not permanently bound documents and bound volumes (books, publications, pamphlets) and other documents that are securely and permanently bound is typed/printed or stamped together at the bottom (preferably in the middle) of every page (including the cover).

11.3. Copies, tracing, photographs, drawings, sketches, etc.

11.3.1. Security classifications should be indicated on such copies, photographs, sketches, etc. by means of rubber stamps. The exact position of the mark may vary, depending on the nature of the document, so that the stamp does not obscure essential details. An effort must, however, be made to mark the document as clearly as possible, so that the mark will immediately attract attention.

11.3.2. Tracings or blueprints should be marked in such a way that the security classification is visible on all copies. Where this is not possible, rubber stamps should be used to mark all the copies.

11.3.4. In case of tape recordings, certain photographs and negatives where, it is physically impossible to place clear classification marks on a documents itself, the document should be placed in a suitable box, envelope or other container and if necessary, sealed, and the nature and classification of the contents clearly marked on the outside of the container.

11.3.5. Files: A clear distinguishing mark, the significance of which is known to those

who deal with the file concerned should be placed on both the front and the back cover of Secret or Top Secret files.

11.3.6. Unclassified sensitive document(s) received from any institution for the use or storage within the Provincial Government must be classified accordingly by the first receiver and be treated subsequently according to the classification marked.

11.3.7. Where necessary, the author of such document as explained must be consulted for more information before the document is graded.

11.4 Access to Classified Information

11.4.1 The general rules and prescriptions as to who may have access to or in respect of classified matters are as follows: -

a. Persons who have appropriate security clearance or who are by the way of exception authorised thereto by the Head of the Department or his/her delegate, with due regard being paid to the need-to-know principle.

11.5. Bulk Conveyance of Classified Documents

11.5.1 **Note:** when classified documents have to be conveyed in bulk by road, rail or air, the appropriate precautions must be taken for the protection thereof.

11.6. Storage of Classified Documents

11.6.1 Classified documents that are not in immediate use must be locked away in a safe storage place according to classification level

a. **Confidential:** Reinforced filing cabinet
b. **Secret:** Strong room or reinforced filing cabinet
c. **Top Secret:** Strong room, safe or walk-in safe

11.7. Removal of Classified Documents from Premises

11.7.1 Classified material may not be taken home without the written approval of the Head of the Department or her/his delegate. A list of the documents to be removed must be handed to the person in control of record keeping. Persons may take classified documents home only if they have proper lock up facilities (see prescribed facilities for the various classified documents), in other words, if a person has no such

facilities, the documents may not have kept at such a person's home for the purpose of work after hours.

11.7.2 Classified documents taken out of building with a view to utilisation at meetings or appointments must be removed in a lockable security attached case. Furthermore, all guidelines mentioned above apply in this regard.

11.7.3. Any departmental official travelling abroad with a laptop issued by the employer should firstly seek approval from the Head of Department.

11.8 Typing of Classified Documents

11.8.1 Only officers having the appropriate security clearance may type classified documents. Such typing must be done in manner that will ensure that the information is not divulged to unauthorised persons.

11.8.2 Draft of classified documents, typewriter ribbons, and copies and floppy disks must at all times be treated as classified documents.

11.9. Destruction of Classified Documents

11.9.1 In terms of the Archives Act, 1996 (Act No.43 of 1996), all documents received or created in a Government Office during the conducting of affairs of such offices are subject to the Act, except where they are excluded due to their very nature of the prescriptions of some or the Act of Parliament.

11.9.2 It should be noted as a point of departure that all state documentation is subject to the Archives Act, unless justifiable excluded along the above-mentioned lines. It should be noted that no document is to be excluded merely because it is classified. The Head of Department will have to decide, after consultation with the Legal Advisors as well as the Director: State Archives whether the document(s) concerned is/are of such a nature that there is a legitimate demand for secrecy that goes beyond the degree of safekeeping by the State Archives.

119.3 Where destruction has been properly authorised, it should take place by burning or some other approved methods, e.g. by means of a shredder (in the latter case – preferably a cross-cut machine), in which case the tips may be not wider than 1,5mm. The person who has destroyed the documents must provide a certificate of destruction of the documents concerned to the Head of the Department or Security Manager.

11.10. Making Photocopies of Classified Documents

11.10.1 All mechanical/electronic reproduction appliances should be properly controlled to prevent the unauthorised or controlled copying or classified documents. This apparatus must therefore either be centralised or distributed and be under the direct control of an authorised and aptly cleared officer.

11.10.2 The relevant programmes must keep a record of all the reproductions of classified documents at its disposal. The register must contain the following particulars; Date, Person requesting copies/reproduction, Classification, File reference, Heading/nature of documents, Purpose of the copies, Number of Copies, Meter readings before and after copying.

12. COMMUNICATION SECURITY

12.1 Personnel Communication

12.1.1 In terms of the Protection of Information Act, 1982 (Act No.84 of 1982) all personnel who potentially have access to classified information are required to sign a prescribed declaration of secrecy, which prohibits the unauthorised release of official information.

12.1.2 All personnel appointed in terms of the Public Service Act, 1994 (Proclamation 103 of 1994) must note and adhere to Regulation II E of the Public Service Regulation, 2001 that deals with the handling of official information and documents: "An employee shall not release official information unless she or he has the necessary authority".

12.1.3 Due cognisance must also be taken to the provisions of the Promotion of Access to Information Act, 2000 (Act No.2 of 2000).

12.2 Communication with the aid of communication equipment

12.2.1 No classified information may be conveyed via telephone, fax, cellular phone or any other communication equipment/aids unless both the sender and receiver use appropriate encryption equipment. The Security managers will co-ordinate the acquisition and maintenance of Security equipment.

12.2.2 Communication security equipment will be acquired from and maintained by the

South African Communication Security Agency as nationally designated sole provider of such equipment.

12.3 Technical Surveillance Counter Measures (TSCM)

12.3.1 Offices, Boardrooms and other places where classified matters are discussed should, apart from effective access control, be secured by means of periodic technical/electronic surveillance counter measures ("electronic sweeping")

12.3.2 The need for and frequency of such measures will be determined by the Head of Department in writing and must provide specific authorisation.

12.3.3 All technical/electronic surveillance counter measures will be executed only by the SSA or any person/institution designated by the SSA in writing.

14. EXCEPTIONS

No exceptions will be allowed in terms of the applicable provisions of this policy.

15. COMMUNICATING THE POLICY

The Security Manager will be responsible for communicating the policy to all stakeholders. The following channels will be used:

a. Information sessions
b. Induction sessions of new employees
c. Booklets, pamphlets and billboards

16. MONITORING COMPLIANCE

16.1 Compliance with the implementation of this policy will be monitored by physical and information security audits on a quarterly or *ad hoc* basis. Heads of Department may request the SSA to conduct security audits at his/her Department, or specific components thereof, to determine compliance with security policies and the state of preparedness.

17. BREACHES OF SECURITY AND REPORTING CHANNEL.

17.1 The security manager must investigate security breaches and recommended remedial actions, including preventative measures and possible disciplines actions where appropriate.

17.2 All criminal related incidence shall be forwarded to SAPS for criminal investigation.

17.3 Incidences related to compromise of information shall be forwarded to the State Security Agency for investigations.

17.4.Loss of assets should be reported immediately to the Director Assets management as well as Deputy Director Security for investigation and necessary action.

18. DEFAULT

Any person contravenes or fail to comply with this policy there shall be progressive intervention.

19. INCEPTION DATE

The inception date of this policy will be effective from the date of approval

20. TERMINATION AND REVIEW POLICY

This policy will be reviewed after three (3) years or if there are new developments or changes in legislations.

21. ENQUIRIES

Any enquiries related to this policy should be forwarded to the Director: Auxiliary Services.

MME. RAKGOALE C. N
MEMBER OF THE EXECUTIVE COUNCIL

31/03/2023
DATE