



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

PROVINCIAL TREASURY

LIMPOPO PROVINCIAL TREASURY

SECURITY POLICY

Table of Contents

ACRONYMS.....	4
1. INTRODUCTION.....	5
2. PURPOSE AND OBJECTIVES OF THE POLICY.....	5
3. AUTHORITY OF THE POLICY.....	6
4. SCOPE OF APPLICATION.....	6
5. LEGISLATIVE REGULATORY FRAMEWORK.....	6
6. DEFINITIONS.....	7
7. POLICY PRINCIPLES.....	11
8. ROLES, RESPONSIBILITIES AND POWERS.....	11
8.1. HEAD OF DEPARTMENT.....	11
8.2. SECURITY MANAGER.....	12
9. EXTERNAL SECURITY STRUCTURES.....	12
10. POLICY PROVISIONS.....	13
10.1 PHYSICAL SECURITY.....	13
10.1.1 Security Appraisals/Surveys.....	13
10.1.2 Access Control (Principles of Access Control).....	14
10.1.3 Key Control and Combinations Locks.....	18
10.1.4 Safe Custody of Safes and Strong room Keys.....	19
10.1.5 Safe Custody of Duplicate Safe/Strong room Keys.....	19
10.1.6 Setting of Combinations: Combination Safes.....	19
10.1.7 Office Security Principles.....	19
10.1.8 Security of Computer Laptop/Desktop.....	20
10.1.9 Maintenance Services of Resources.....	21
10.1.10 Asset Control and Removal of Departmental Property.....	21
10.1.11 Private Security Services.....	21
10.1.12 Security Registers: Private Security Service Providers.....	22
10.1.13 Reports of Losses.....	22
10.1.14 Security Awareness.....	22
10.1.15 Security Appraisal in Departmental Buildings and Sites.....	23
10.2 DOCUMENT SECURITY.....	23
10.2.1 Classification of Information.....	23
10.2.2 Confidential Classification Test.....	24
10.2.3 Secret Classification Test.....	24
10.2.4 Top Secret Classification Test.....	24
10.2.5 Access to Classified Information.....	25
10.2.6 Handling of Classified Information.....	26

10.2.7	Minimum Safe Storage Requirements: Classified Documents.....	26
10.2.8	Removal of Classified Documents.....	26
10.2.9	Typing of Classified Information.....	26
10.2.10	Photocopying of Classified Documents.....	27
10.2.11	Sealing of Classified Documents before Dispatch.....	28
10.2.12	Destruction of Classified Documents.....	29
10.2.13	Transmitting Classified Documents By Means Of Facsimile.....	29
10.2.14	Securing of Classified Documents.....	30
10.2.15	Record-Keeping of Classified Documents.....	31
10.2.16	Registries and Files.....	31
10.2.17	Central Registries for Receiving and Dispatching Mail.....	32
10.2.18	Access to Main Registry.....	32
10.2.19	Management of Files.....	32
10.2.20	Sealing of Classified Documents and Courier Services.....	33
10.2.21	Transmitting Information by Computer.....	34
10.2.22	Removal of Classified Documents from Premise.....	34
10.2.23	Destruction of Classified Documents.....	36
10.2.24	Meetings.....	37
10.2.25	Security Inspection of Files Containing Classified Documents and Registers Referring to the Position of Such Information.....	37
10.2.26	Handling of Classified Information in Emergency Situations.....	37
10.2.27	Loss of Classified Information.....	38
10.2.28	Security Marking of Documents.....	38
10.2.29	Documents and Bound Volumes.....	38
10.2.30	Copies, Tracings, Photographs, Drawings, Sketches.....	38
10.2.31	Rolled or Folded Documents.....	38
10.2.32	Tape Recordings and Documents on Which No Marks Can Be Made.....	38
10.2.33	Contingency Planning: Document Security.....	39
10.2.34	Reporting of Incidents which may Influence a Person's Security Competence.....	39
10.3	PERSONNEL SECURITY.....	40
10.3.1	Personal Suitability Checks.....	40
10.3.2	Vetting Criteria.....	41
10.3.3	Security Screening In Respect of Immigrants and Officials with more than One Citizenship.....	41
10.3.4	Screening of Officials Who Have Lived/Worked Abroad For Long Periods.....	43
10.3.5	Security Screenings of Contractors Supplying Services to the Department.....	43
10.3.6	Period of Validity of Security Clearances.....	44

10.3.7	Transferability of Security Clearances.....	44
10.3.8	Responsibilities of the Screening Authority.....	44
10.3.9	Responsibilities of the Head of the Department With Regards to Security Clearances.....	45
10.3.10	Responsibilities of Officials Travelling Abroad on State Missions.....	46
10.4	COMMUNICATION SECURITY.....	46
10.5	TECHNICAL SURVEILLANCE COUNTER MEASURES (TSCM).....	47
10.6	INFORMATION SECURITY.....	47
10.5.1	Responsible Use: Ethics in Computer Usage.....	47
10.5.2	Measures to be implemented.....	48
10.6	CRYPTOGRAPHIC SECURITY.....	48
10.6.1	Cryptography.....	48
10.6.2	Cryptographic Security Compromise / Violation.....	48
10.6.3	Chief Communications Officer.....	49
10.6.4	Clearance of Personnel Utilising / Managing Cryptographic Equipment.....	49
10.6.5	Cryptographic Custodians.....	49
10.6.6	Responsibilities of Primary and Secondary Custodians.....	49
10.6.7	Maintenance of Cryptographic Equipment.....	50
10.6.8	Compromises and Violations.....	50
11.	DEVIATION.....	50
12.	COMMENCEMENT DATE.....	50
13.	TERMINATION AND REVIEW CONDITIONS.....	50
14.	ENQUIRIES.....	51
15.	RECOMMENDATION AND APPROVAL.....	51

ACRONYMS

COMSEC	-	Communications Security
IT	-	Information Technology
LPT	-	Limpopo Provincial Treasury
MISS	-	Minimum Information Security Standards
PSC	-	Personnel Suitability Check
RSA	-	Republic of South Africa
SACSA	-	South African Communication Security Agency
SANDF	-	South African National Defence Force
SAPS	-	South African Police Service
SASS	-	South African Secret Service
SSA	-	State Security Agency
MPL	-	Member of Parliament
MPSS	-	Minimum Physical Security Standards
HoD	-	Head of Department

1. INTRODUCTION

- a) Security today requires more than the traditional concepts of guards and alarm systems to protect and serve business continuity and service delivery. Modern organisations, which include the government services, are increasingly being threatened by ever more complex acts of crime, accidents, natural disasters and theft of proprietary information. Accordingly, the emphasis must be on a systematic and logical approach to known and potential threats and security vulnerabilities within the department.
- b) A comprehensive approach to security not only protects personnel, information, clients but assets, facilities and the core business function of the department, as embodied in the Mission and Vision of the department.
- c) The security division is not designed to replace public law enforcement or other security agencies, but rather to compliment the efforts of a multi-disciplinary approach by government, to prevent and control the risks, crime and security breaches that the department is or could be exposed to.
- d) While the security division is prevention oriented in providing cost effective solutions to security problems, there can be no effective security condition in the department without the following requirements:
 - i) Security standards and institutionalised policy on security;
 - ii) These standards should form part of a comprehensive system of security measures;
 - iii) These measures must be properly managed;
 - iv) These measures must be adhered to and enforced, and
 - v) Personnel must be security–conscious.
- e) This policy document contains guidelines aimed at protecting the people, interests, liabilities, assets, activities, classified matters and risk exposure of the department. The document further provides the minimum standards for providing a condition of security and safety in the department.

2. PURPOSE AND OBJECTIVES OF THE POLICY

- a) The objective of the policy is to develop and provide progressive security programs and measures to meet the following objectives:
 - i) Maintenance of a safe and secure workplace,
 - ii) Ensure employee safety and security,

- iii) Protection of departmental assets and information,
 - iv) Reduction of security related risks and losses,
 - v) Proactive management of liabilities,
 - vi) Ensure business continuity of the department.
- b) The security policy will complement the established departmental contingency plan. If plan not developed, it shall be developed concurrently with the security procedures, in collaboration with the transformation services division.
- c) The security division will provide security procedures and implementation plan after approval of the policy.
- d) Security standards will be developed to ensure quality assurance and standardization of security services, equipment and practices.

3. AUTHORITY OF THE POLICY

This policy is issued under the authority of the MEC as the Executive Authority and the Head of Department as the accounting officer for the department.

4. SCOPE OF APPLICATION

This policy applies to all employees, contractors, consultants as well as any other individuals conducting business or visiting the department and will be subjected to these provisions set out in this document.

5. LEGISLATIVE REGULATORY FRAMEWORK

NO	DESCRIPTION
1.	Bill of Rights Act (Act No.108 of 1996)
2.	Civil Protection Act (Act NO. 67 of 1977)
3.	Control of Access to Public Premises and Vehicles Act (Act NO. 53 of 1985) (As amended)
4.	Criminal Procedures Act (Act No. 51 of 1977)
5.	Fire Brigade Act (Act No. 99 of 1987)
6.	Firearms Control Act (Act No. 60 of 2000)
7.	Hazardous Substances Act (Act No. 15 of 1973)
8.	Labour Relations Act (Act No. 66 of 1995)
9.	National Key Point Act, 1980(Act No. 102 of 1980)
10.	Law of Evidence Act (Act No. 25 of 1965)

NO	DESCRIPTION
11.	Minimum Information Security Standards (MISS) Policy document(Approved by Cabinet on 4 December 1996)
12.	National Building Regulations and Building Standard Act (Act No. 103 of 1977)
13.	Occupational Health and Safety Act (Act No. 85 of 1993)
14.	Private Security Industry Regulatory Act (Act No. 56 of 2001 and Regulations thereto)
15.	Promotion of Access to Information Act (Act No. 2 of 2000)
16.	Protection of Information Act (Act No. 84 of 1982)
17.	Public Finance Management Act (Act No.1 of 1999)
18.	Public Service Act (Act No. 1994)
19.	Public Service Regulations, 1996
20.	Private Security Industry Regulatory Act (Act no 56 of 2001 and Regulations thereto.)
21.	Treasury Regulations for Departments, Constitutional Institutions and Trading Entities (Government Gazette No. 21249 dated 31 May 2000.)
22.	Minimum Physical Security Standards (MPSS)
23.	Trespass Act (Act No. 6 of 1959)

6. DEFINITIONS

a) ACCESS CONTROL:

The process and measures by which access to and exit from a government building/facility/premises are controlled or restricted. The authority for these measures is outlined in the **Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985)** as amended.

b) ACCESS CONTROL CARD:

A card issued in accordance with government directives to a qualifying person subject to certain conditions, allowing that person access to specific areas.

c) AUTHOR (ORIGINATOR OF DOCUMENTS):

Any person acting on behalf or in the interest of the state whether employed by the state or not, but who generates or prepares a document whether it is classified or not.

d) CLASSIFIED INFORMATION:

Information that is regarded as sensitive in terms of the activities of the government, and must by reason of its sensitive nature be exempted from disclosure and

therefore enjoy protection against compromise. Such information is classified as **Confidential, Secret or Top Secret**.

Remark: "Information" used as a descriptive term in this security policy refers to all forms of communication, that is, verbal, written, magnetic or electronic. "Activities" of the government refer to any design, development, product, planning, cooperation or function of a proprietary nature.

e) **CLASSIFY/RECLASSIFY:**

The grading/categorising or regarding/re-categorising of information, in accordance with its sensitivity or in compliance with a security requirement.

f) **COMMUNICATION SECURITY:**

That condition created by the conscious provision and application of security measures for the protection of classified information communicated through electronic means, ensuring that the confidentiality, integrity, accountability and authentication of data during and after transmission is maintained.

g) **COMPROMISE:**

The unauthorised disclosure/exposure/loss of classified information; or information qualifying for classification; or exposure of sensitive activities, people or places, whether by design or through negligence.

h) **CONTINGENCY PLANNING:**

The prior planning of any steps that has the purpose to prevent and/or combat, or counteract the effect and results of an emergency situation where lives, property or information of the government is threatened. This includes compiling, approving and distributing a formal, written plan, and practising this, in order to identify and rectify gaps in the plan, and to familiarize staff and coordinators with the plan.

i) **CONTRACTOR:**

Any institution/service provider or member thereof, who provides a specific service as contractor or sub-contractor.

j) **COPYING:**

The making of a copy of information (irrespective if in document, mechanical or electronic format), whether by copying it out by hand, by photographic means, audio recording, electronic or any other means.

k) **CRYPTOGRAPHIC SECURITY:**

To prevent any possibility of unauthorised decryption of coded information and is achieved by the provision of secure cryptographic systems and their correct usage.

l) **CRYPTOGRAPHIC SECURITY COMPROMISE/VIOLATION:**

Cryptographic security compromise or violation occurs whenever unauthorised persons gain knowledge or intercept messages and /or material and equipment related to the crypto environment.

m) **DOCUMENT:**

In terms of the Protection of Information Act (Act 84 of 1982) a document is:

Similar process;

- Any copy, plan, picture, sketch or photographic or other representation of any place or article;

- Any disc, tape, card, perforated roll or other device in or on which sound or any signal has been recorded for reproduction.

n) **DOCUMENT SECURITY:**

That condition which is created by the conscious provision and application of security measures in order to protect documents with sensitive contents.

o) **HEAD OF DEPARTMENT:**

The person who is serving as the head of a department, as defined by law, directive or otherwise, including the official acting in his /her place.

p) **IDENTIFICATION:**

The identification of a person for the purpose of access to a security area (that is, an area that is being secured by security regulations because of activities that necessitate such measures), which entails positive recognition through a government identification card, a national identity document, a passport or similar document, or by physical identification through another identified and known government employee.

q) **INFORMATION:**

Information is any recorded or displayed data or knowledge or content of communication, regardless of its format.

r) **INFORMATION SECURITY:**

That condition created by the conscious provision and application of a system of document, personnel, physical, information technology and communication security measures to protect classified and sensitive information.

s) **INSTITUTION:**

"Institution" means any department of the state, body or organisation that is subject to the Public Service Act, or any other law or any private undertaking that handles information classifiable by virtue of national interest.

t) **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, normally in accordance with that person's level of security competence/clearance.

u) **PERSONNEL SECURITY:**

Personnel security is that condition created by the conscious provision and application of security measures in order to ensure that any person who gains access to classified information or information of a sensitive proprietary nature does have the necessary security grading or proof of security competence (irreproachable trustworthiness), and conducts him/herself in a manner not endangering him/her or the compromise of classified / sensitive information.

v) **PHYSICAL SECURITY:**

That condition which is created by the conscious provision and application of physical security measures for the protection of persons, property, information and liabilities.

w) **SECURITY:**

That condition free of risk or danger to lives, property and information created by the conscious provision and application of protective security measures.

x) **SECURITY CLEARANCE:**

An official document that indicates the degree of security competency of a person. This document is normally issued by vetting institutions e.g. SSA, SASS, SAPS, SANDF and any other institution that has been mandated by an act of parliament or other policies to do so.

y) **SECURITY COMPETENCE:**

Persons ability to act in such a manner that he does not cause classified information or material to fall into unauthorised hands, thereby harming or endangering the

security or interest of the state. It is normally measured against the following criteria, namely: susceptibility to extortion or blackmail, amenability to bribes and susceptibility to being compromised due to compromising behaviour and loyalty to the state or department.

z) SECURITY MANAGER:

The head of the Security division, responsible for provisioning of security and investigation services within the department.

aa) SECURITY VETTING:

The process followed to determine whether a person is able to maintain confidentiality and whether his/her trustworthiness is without reproach. It includes the person's ability to handle information of a classified or proprietary nature in such a manner that he/she does not cause this information or material to fall into unauthorised hands, thereby harming or endangering the interests of government or the Republic of South Africa.

bb) STORAGE:

The safekeeping of classified documents in appropriate (as prescribed) lockable containers, strong rooms, record rooms and reinforced rooms.

7. POLICY PRINCIPLES

7.1 GUIDING PRINCIPLES:

- a) Client centred
- b) Accountable for quality results
- c) Inspired and innovative

7.2 CORE VALUES:

Personal commitment, honesty and integrity.

8. ROLES, RESPONSIBILITIES AND POWERS

8.1. HEAD OF DEPARTMENT

- a) The head of the department as accounting officer bears the overall responsibility for the provision and maintenance of security in his/her department.
- b) Apart from the ordinary or customary powers of delegation to senior officers or employees, the head of department will ensure that a clearly formulated security policy of the institution is in place in order to maintain information security and to ensure physical security standards. He/she must ensure that the

security function is delegated in writing to a fit and proper officer/employee and provision shall be made for the effective administration and practice of security.

- c) The head of department must ensure that a security policy provides in unambiguous terms the powers, responsibilities and duties of the security staff, and must require all personnel to submit to security measures. Security being an integral part of the management function, the composition of the security division must be such that the line of authority does not obstruct access to the head of department and top management.

8.2. SECURITY MANAGER:

- a) The security manager is responsible for all aspects of security and Investigations and shall develop and implement security programs in coordination with top management, the risk and security management committee.
- b) The security manager will investigate all security breaches (losses) with security implications involving departmental property, classified/ sensitive information or personnel.
- c) The security manager will assist other law enforcement agencies (SAPS, SSA, and COMSEC) with investigations related to possible corporate crime, security breaches or incidents involving departmental property or personnel.
- d) The security manager, in consultation with the head of department will, appropriately, report to law enforcement agencies and other state department institution in terms of the law, any criminal violations and security breaches with regard to departmental personnel, property and information.
- e) The security manager will provide operational policies and procedures to all managers and supervisors.
- f) The security manager must establish a security committee consisting of representatives of various directorates in the department and chaired by him/her.
- g) The purpose of security committee is to ensure that proper security measures in accordance with all relevant legislative requirements are implemented to prevent the loss of production and ensuring that the integrity of the department is upheld.

9. EXTERNAL SECURITY STRUCTURES:

A number of departments/institutions have been appointed custodians of certain specific security functions and responsibilities on national and provincial levels.

The responsibilities are allocated as follows:

Institution	Responsibility
COMSEC under State Security Agency (SSA)	Communication Security(Cryptography)
State Security Agency (SSA)	Computer Security
State Security Agency (SSA)	Information Security
State Security Agency (SSA)	Personnel Security
South African Police Service (SAPS)	Physical Security
South African Police Service (SAPS) and State Security Agency (SSA)	Security Training

10. POLICY PROVISIONS

10.1 PHYSICAL SECURITY

10.1.1 Security Appraisals/Surveys

- a) Physical security evaluations will include the designation of security areas/security zoning, increasing in the degree of protection and protective layers provided at the facility, starting from the perimeter (outside) to the inner part of the premises/facility and identified security zones/sensitive areas.
- b) Security involves the development of a cost-effective approach to reduce the exposure to security risks.
- c) Prior to the implementation of physical security measures/equipment, a formal appraisal or survey shall be conducted at the identified premises to determine the following;
 - i.Mission and core function of the unit / facility;
 - ii.The current security status of the premises under review,
 - iii.Identify deficiencies or security risks,
 - iv.Define the protection needed, and
 - v.Recommend measures to minimize the security exposure/vulnerability/threat.
- d) The level of security required will be determined by the crime rate of the area, incident reports, risk exposure and the existing physical security. (fencing, alarms, burglar, guarding services, illumination etc).
- e) All security requests/ needs must be directed to the security manager for his/her attention.

10.1.2 Access Control (Principles of Access Control)

a) Persons Requiring Access Must Be Identified

- i) Positive identification must be provided at all times, prior to authorising entry to the facility - RSA identity book, driver's licence, passport, departmental access card, SAPS or SANDF appointment certificate).
- ii) When positive identification is not possible, an employee known to the authorising officer can identify the visitor.
- iii) Due to the inherent deficiencies of this method, record must be kept of the visitor and the person visited or host. Relevant registers must be provided by the private security service provider at the site where deployed. It is the responsibility of the security service provider at the site to enter information of the visitor(s) using relevant documentations before access can be granted. Visitors must be escorted to the host, from rank of senior manager; other hosts must collect their visitors at the security reception. The host accepts the responsibility and must ensure that the person is escorted back to the security reception. The host shall be informed by telephone of the intended visit and collection at the security reception. It is the responsibility of the host to hand back the visitor to security reception.

b) Acceptable Reason for Visit

- i) The visit must relate to official business of the department or host being visited.
- ii) Visits by friends and family should be minimized.
- iii) Hawkers, persons selling novelty items or requesting humanitarian contributions that have no official business at departmental premises may not be allowed to enter any premises of the department. Any item ordered by personnel in their private capacity must be collected directly from the supplier. The security personnel will contact the employee by internal telephone for the collection of the items. Where the individual is not available or cannot be contacted, acceptance of the goods will be refused. Payment and receipt for the goods is the responsibility of the person requesting the service. The security personnel will not be involved with payments and will not accept any responsibility for these items.
- iv) Maintenance personnel or external service providers must be cleared as being on official business, prior to access being granted. The clearance should include contacting the employer and confirming their official business at the premises as well as confirming with auxiliary services division that the services have been requested. The required registers must be completed with particulars of individuals.

c) Authorisation to Enter Premises

- i) An official departmental access card or identification sticker provides authority to enter the premises. Visitor cards or stickers will be identified with "VISITOR" imprinted thereon. Where a person is found on the premises without an official personnel or visitor card or sticker, confirmation of being an authorised government official or visitor at the premises should be obtained. Where no prior authority was provided for visitors, the required register must be completed and authority to enter the premises be considered.
- ii) The card/sticker must be carried in full view by way of a lanyard around the neck or pasted on the chest.
- iii) Persons having no official purpose or reason to enter the building should be denied access for security reasons and to reduce the risk exposure of the department.

d) Declaration/Search of Visitors

- i) Security officers do not have the statutory authority to physically search a person(s). These searches may however be conducted if authorised in terms of section 2 (2) (g) of the Access to Public Premises and Vehicles Act, Act 53 of 1985.
- ii) Section 2 (2) of the Act however authorises the request for an obligation by the visitor to provide identification and the declaration of any prohibited items or contents of any dangerous weapon, suitcase, briefcase, handbag, parcel under his/her control, and the provision of information, as required by the registers in use.
- iii) Persons who refuse to:
 - Submit to an electronic search (security x-ray equipment).
 - Provide the required information.
 - Have security personnel inspect the item(s) under their control, should be denied access to the premises and the matter be reported to the Security division. Under no circumstances should the person be forced to submit to a search, should they refuse.
- iv) Should any unauthorised object be found under the control of the visitor, the item must be retained at security reception, registered and reported to the security division for investigation and transfer to the South African Police Service, where applicable.
- v) Searches of personnel or persons who leave/exit the premises should be a condition of authority to enter the building or working at the premises. While a person cannot be forced to subject to a search when leaving the building in accordance with the **Control of Access to Public Premises and Vehicles Act, 53 of 1985**, such a person can be detained if he/she refuses, with the

proviso and the security official has a **reasonable suspicion** that the person was involved in any action on the premises that constitutes a crime. Any incident of this nature must be reported to the security division for investigation and coordination of possible action by the South African Police Service.

- vi) The searching of people entering the premises is sensitive and should be treated with care, dignity and respect to the person being searched.
- vii) The Criminal Procedure Act must be complied with regarding the search of women by women and male by male.

e) Illegal/Unauthorised Items

- i) Any firearms, dangerous weapons, any item that could cause the reasonable suspicion that it may be used to cause damage or injury to any person is viewed as illegal and unauthorised items.
- ii) No firearms may be allowed on identified premises of the department. The only exceptions are members of the South African Police Service, South African National Defence Force, Correctional Services, and State Security Agency while visiting/entering the building on official duty/purpose only. Members of the Security division as well as officials of a private security services providing contract services at the premises are allowed to have firearms in their possession, while on departmental premises.
- iii) Firearms must be registered by the security officers and secured in a two-key gun safe or other authorised security device by the owner/user thereof. The authorised owner/user must personally retrieve the firearm from the safe or device, sign for receipt thereof, when exiting the premises. No firearm may be handled in any way by the security officers or any person other than the authorised owner/user thereof. Firearms may not be made safe during these transactions to minimise the risk of injury or damages. The owner/user is familiar with the firearm and therefore the handling thereof personally when securing and retrieving the firearm. Where firearms are secured the firearm licence or permit must be perused and particulars thereof registered.
- iv) Depending on the specific functional circumstances of the premises, some building of the department may require that firearms be handed in, apart from the exceptions mentioned, at the security reception as stated above. These buildings will be indicated as such with "no firearms" signage.
- v) All vehicles entering a secured official parking area of the department may be searched when entering or leaving the premises.
- vi) Only authorised vehicles may enter the official parking area.

- vii) Standard warning signs must be posted at all departmental premises with regard to: "no trespassing, per order of the department" imprinted on the sign.
- viii) Signs should also be provided at the access control points, indicating: "right of admission reserved", "access control enforced at the premises", close circuit television is deployed at this premise".
- ix) Control of Access to Public Premises and Vehicles Act, Act 53 of 1985 is applicable to these premises".

f) Keeping of Records

- i) A complete record of all visitors as well as personnel visiting departmental premises during and after hours must be kept. An afterhours register must be maintained by the security officers. (While access card system will record authorised visits, the access still must be monitored).
- ii) The record serves as authority being provided to enter the premises and tracking of these visits.

g) Setting of Conditions

- i. Access to departmental premises is subsequent to conditions being applied, as mentioned in **Section 2 (3) (a) of Act 53 of 1985**.

h) Escorting

- i) All visitors shall be escorted, either by security officers/host within the premises.
- ii) Security officers are required to escort deliveries, contractors and technicians, while on the premises. Officials responsible for maintenance at the departmental premises shall make arrangements for the escorting of these contractors and technicians, where these services provided on the premises take longer than 30 minutes. Where possible, the office users must supervise maintenance in their offices. Should this not be possible, arrangements must be made for direct supervision. All documents must be secured when these services are provided.
- iii) Visitors to facilities, identified as security/sensitive areas, shall be escorted to the specific offices by the security officers where after the secretary, host or supervisor must arrange for the exit of the visitor.

i) Limited Access Control Areas

- i) Limited access control areas may be located within the protected area. Such areas will be clearly identified and secured to prevent unauthorised access.
- ii) Tailgating is forbidden.

- iii) Using of some one's access card to gain access to the building is prohibited.
- iv) Trespassers will be prosecuted.
- v) Access control report and CCTV footages will be regarded as the true reflection of the individual movement record within the building, unless proven otherwise.

j) Deactivation of terminated employees on access control system

- i) HRM to issue supervisor/employee with clearing out form, the form is provided to security and investigation services.
- ii) On the last day of office, the SIS will request all department keys, access card and access rights of the employee will be revoked from the system.
- iii) The employee will be treated as a visitor thereafter for any visit to the department whereby visitor's register will be completed.

10.1.3 Key Control and Combinations Locks

- a) A key custodian must be appointed at all departmental buildings to manage and control the provision of keys, maintain records and registers and conduct regular inspections regarding compliance with the key control directives and procedures.
- b) A key control system must be implemented at all departmental facilities and key users must sign a register for the key(s).
- c) Master keys must be kept with the security division, for use in emergencies only and the use thereof noted in the applicable register(s). The master keys must be secured in sealed security key bags and held in a safe or strong room.
- d) Duplicate keys, managed by the key custodian, must be secured in a key safe and the required use thereof noted in the applicable register(s).
- e) Duplication of keys may only be done by key custodian (no one else) with the permission of the security manager, (head of Security division).
- f) The access card provided to personnel is also viewed as being a key and is part of the key control system.
- g) Keys are provided free of charge. Any loss of key must immediately be reported to the security manager accompanied by a statement on how the key was lost. The key custodian will replace any key lost and/or lock replacement and recover the cost from the user.
- h) The key system of the departmental buildings must comply with master key principles. Where these do not exist, the system must be phased in.
- i) Employees who resign or relocate from offices must return the keys to the key custodian. No keys may be transfer among the employee without the permission from the security division.
- j) Before an official can occupy a new office, locks must be changed.
- k) Keys are issued as per procedure manual.

10.1.4 Safe Custody of Safes and Strong Room Keys

- a) The transfer of a safe to another office or when a safe is purchased must be reported to the key custodian, auxiliary services and security divisions.
- b) The primary user of the safe or strong room is responsible for the safekeeping of the key/s. Any loss of the key(s) must immediately be reported to the Security division or key custodian.

10.1.5 Safe Custody of Duplicate Safe/Strong room Keys

- a) Duplicate safe and strong room keys must be provided to the security division for safekeeping. These Keys are kept in a sealed security key bag, for use during emergencies only. A written request must be provided prior to the provisioning/issue of the duplicate key by the security division. An investigation will be conducted into the loss and circumstances thereof.
- b) Keys that are lost must immediately be reported to the key custodian and security division, for the necessary investigation and risk management measures. The lost key/s will be paid as per government global tariffs.
- c) Safe and strong room keys may not be placed in desk drawers but kept on the person while on duty. The key must be secured in a steel cabinet or drop in safe at the security reception when not in use.

10.1.6 Setting of Combinations: Combination Safes

- a) Safes fitted with combinations locks must be reset under the following circumstances:
 - i) When purchased,
 - ii) When suspected of being compromised,
 - iii) When a new user takes over the safe,
 - iv) On resumption of duty when absent for long period of time due to vacation leave or other official reason, and when the combination has been provided to another person due to an emergency.
 - v) Should the code be forgotten, the user must report to the key custodian to manage to reset the code in the present of the user.

10.1.7 Office Security Principles

- a) Each employee of the department is responsible for the security of his/her own office.
- b) The door of the office must be locked not closed when absent.
- c) Where more than one official occupy offices, valuable items must be properly secured by owner.
- d) Any suspicious item found on the premises must be reported to the security division immediately.

- e) Employees shall be individually responsible for the security of their personal properties. The department will not accept any responsibility for personal properties.
- f) The cleaning of offices and maintenance must take place under supervision of the office occupants.
- g) The air-conditioner and other electric devices/appliances must be switched off when leaving the office at the end of the day.
- h) No sensitive or classified document may be left on desks when not in use. These documents must be locked away in the prescribed facilities as per MISS.
- i) Documents that could be viewed as sensitive/classified must be secured when leaving the office/facility at the end of the day.
- j) No visitors must be left unattended in the offices.

10.1.8 Security of Computer Laptop/Desktop

- a) Laptop computers provide a convenient method for conducting business outside the office. Because of their portability, however, they are at significant risk of theft, along with any sensitive information they may contain. Employees must provide an appropriate level of protection for the laptops assigned to them. The following guidelines are intended to assist in that effort:
 - i) When away from workstations for an extended time, remove laptops from docking stations and lock them in desks or filing/storage cabinets. If away for a short time, a cable lock may be used.
 - ii) If laptops are left in the office overnight, they must be locked in a secure place (desk or filing/storage cabinet). A docking station (even if it has a lock) is not considered secure.
 - iii) Provide an appropriate level of protection for laptops when out of the office, lock it away.
 - iv) At home, store laptops out of sight when not in use, or preferably in lockable storage if available.
 - v) Never leave laptops in plain view inside vehicles. If a laptop must be left in a vehicle, place it in the trunk or a locked storage compartment.
 - vi) Never leave laptops unattended in public locations, even for a few minutes. This includes airports, train and bus stations, meeting rooms, hotel lobbies and rooms, etc.
 - vii) If a laptop must be left in a hotel room, place it out of sight in locked luggage or a drawer. If available, make use of in-room or front desk safes as secure storage locations.
 - viii) When breaking for lunch in a meeting room, do not leave the laptop unattended.
 - ix) Never check-in laptops as baggage when using public transport facilities. Departmental laptops are always considered carry-on luggage. Keep laptops in

- sight as they go through airport security screening.
- x) Ensure critical information is backed up regularly, and the backup is stored in a location separate from the laptop. (consult IT division for advise).
 - xi) Consider encryption of any sensitive information stored on laptops (Consult IT Section for advise).
 - xii) Limit taking laptop home after hours and move around with it either by vehicle /foot.
 - xiii) It is the responsibility of the official to register laptop on the applicable register at the security reception when leaving and entering treasury sites.

10.1.9 Maintenance Services of Resources

- a) The office user must supervise all maintenance services, repairs and cleaning of offices. Should this not be possible, arrangements must be made for supervision.
- b) All documents must be secured when these services are provided.
- c) Maintenance services or repair within offices must be verified as being bona fide.
- d) The security division will assist with the verification of these services.

10.1.10 Asset Control and Removal of Departmental Property

- a) Assets (furniture/computer/technical) moved/transferred between offices must be reported to the assets management in writing and reflected on the office/departmental inventory.
- b) The removal of government/departmental property (furniture/computer/technical) from the departmental premises must be authorised by the supervisor in writing.
- c) The security officers will note the item/s, serial numbers, asset numbers and particulars of officials authorised to remove the item/s.
- d) No employee may remove or take away any government or departmental property, without the proper approval.
- e) The item(s) must be declared upon return thereof to the security officers, for accounting purposes.
- f) Theft/loss of government/departmental as well as private property must immediately be reported by telephone and in writing to the security division, for investigation and report to the South African Police Service, where applicable.
- g) **NB:** It is the responsibility of the official moving asset to provide necessary papers before the asset leave the departmental premises.

10.1.11 Private Security Services

- a) Security officers may not be utilised for any other purpose than as stipulated in the contract or service level agreement.
- b) In order to enable the security officers to perform their duties the following equipment may be supplied, after consultation with the security division and in accordance with the security needs of the specific facility:

- i. Security x-ray units / machines,
 - ii. Walk through metal detectors, and
 - iii. Hand held metal detectors.
- c) The outsourced contract specifications will be in an indication of security items to be provided by either the company or department.
- d) The security division will conduct site monitoring and audit outsourced security services with regard to compliance of (Service Level Agreement) service delivery standards and contract specifications.
- e) Any complaints regarding service delivery by these services must be reported to the security manager in writing as soon as possible. Interfering with security officers on duty is forbidden.
- f) The security manager must be consulted regarding the security screening of any envisage contract in the department.
- g) Prior to the services of private security being contracted, the security division will conduct an evaluation/survey of the facility, required service and provide recommendations.
- h) In evaluating the outsourced security requirements, careful consideration will be given to the nature, vulnerability, physical layout of the facility and crime pattern of the area.
- i) The security division will have regular meetings with the outsourced security companies to establish standards of service delivery and address operational matters.

10.1.12 Security Registers: Private Security Service Providers

- a) Private security companies will provide, maintain and complete the required security registers at all departmental facilities where they are employed.

10.1.13 Reports of Losses

- a) The security division has the responsibility to ascertain the risk and threats that the department is exposed to. In order to fulfil this function all managers, supervisors' must report any loss/theft of state/departmental property within 24 hours to security division for an investigation and statistical analysis and update of the risk profile of the department.
- b) All security breaches must be reported to the Office of the Security Manager.
- c) Any act of misconduct and acts that constitutes criminal conduct must be reported to the Office of the Security Manager for investigation and coordination with the South African Police Service, where required.

10.1.14 Security Awareness

- a) Training and circulars will be provided to ensure that all employees are security conscious and aware of their security responsibilities.

- b) All new employees must undertake security induction prior commencing with their respective duties.
- c) All posters/pamphlets before being display on departmental premises shall be approved by communication services division.

10.1.15 Security Appraisal in Departmental Buildings and Sites

- a) Security division is responsible for security appraisals at all buildings and facilities under the control of the department.
- b) Where applicable, the appraisal or survey may be conducted in collaboration with the State Security Agency (SSA), South African Police Service (SAPS).
- c) Office of the Security Manager must be informed well in advance of any intention to acquisition of additional departmental accommodation or relocation of offices, for the required security appraisal.
- d) The provisioning of security equipment must be investigated for inclusion in the lease agreement or tender with the acquisition of newly acquired departmental building or facility.

10.2 DOCUMENT SECURITY

10.2.1 Classification of Information

- a) All divisions which handle on their day-to-day basis information that is to some extend sensitive and obviously require security measures. The level of security grading of information of a sensitive nature is determined by the degree of sensitivity of such information. It is the responsibility of any person who is the author of a document that contains information of a sensitive nature, to classify the document accordingly, as indicated below.
- b) The classification assigned to documents shall be strictly observed and may not be changed without the consent of the author and where the author is not available, the head of department or security manager can assist.
- c) If the receiver of a classified document is of the opinion that the document concerned must be re-classified, he/she must obtain oral or written authorization from the author, the head of the department or security manager. Such an authorization must be indicated on the relevant document when it is re-classified.
- d) The classified document or file will be determined by the highest graded information it contains. The same classification as that of the original must be assigned to extracts from classified documents, unless the author, head of department or security manager consents to a lower classification.
- e) Every document must be classified on its own merit and in accordance with the origin of its contents authors of documents must guard against the under classification, over classification or unnecessary classification of documents.

10.2.2 Confidential Classification Test

- a) Information must be classified as **CONFIDENTIAL** when compromise thereof could lead to:
- i) The frustration of the effective functioning of information and operational systems.
 - ii) Undue damage to the integrity of a person or department or dealing with a department, but not entailing a threat of a serious damage. Compromise of such information, however, can frustrate everyday functions, lead to an inconvenience and bring about wasting of funds.
 - iii) The inhibition of systems, the periodical disruption of administration (e.g. logistical problems, delayed personnel administration, financial relapses, etc.) that inconvenience the department, but can overcome, and the orderly, routine co-operation between institutions and / or individuals being harmed or delayed, but not bringing functions to a halt.
 - iv) The disruption of ordered administration within the department and adverse effect on the operational relations between institutions.

10.2.3 Secret Classification Test

- a) Information must be classified as **SECRET** when the compromise thereof:
- i) Can result in disruption of planning and fulfilling of tasks, i.e. the objectives of a department or institution dealing with the department in such a way that it cannot properly fulfil its normal functions,
 - ii) Can disrupt the operations and co-operations between departments in such a way that it threatens the functioning of one or more of the departments.
 - iii) Can damage operational relations between departments and diplomatic relations between States.
 - iv) Can endanger a person's life.

10.2.4 Top Secret Classification Test

- a) Is used when the compromise of information could result in:
- i) The functions of the Provincial Government being brought to a halt by whatever actions,
 - ii) The severing of relations between States,
 - iii) Could disrupt the effective execution of information or operational planning and/or plans;
 - iv) Can seriously damage operational relations between governments.
 - v) Can lead to discontinuation of diplomatic relations between states or governments and can result in declaration of war.

- b) It is the responsibility of the author / originator of a document to:
 - i) Allocate copy numbers to the document, including to documents distributed as drafts,
 - ii) To establish the distribution list of such classified information, including the principle of an “**Only Copy**” or attaching exclusivity
 - iii) To attach an embargo on making copies or extracts, should it be necessary.

- c) The number of copies, including the number of the particular document, should be clearly indicated on the first page in the right-hand corner, for example, copy one of three copies. At the end of the message after the signature block, the distribution of these copies should be indicated, for example:
 - i) Copy One (1) of Three (3) Copies: The Director General
 - ii) Copy Two (2) of Three (3) Copies: The Head of the Department
 - iii) Copy Three (3) of Three (3) Copies filed in file XYZ.

- d) Should the possibility of future reclassification exist, that is, after a certain period or upon the occurrence of a particular event, it must be indicated.

- e) Situations could arise where documents are received from external institutions or a government department, which already bears a security classification. When this classification implies particular handling or limiting normal access, such documents must be handled accordingly.

10.2.5 Access to Classified Information

The rules and prescriptions as to who may have access to or inspect classified matters are as follows:

- a) A person who has an appropriate security clearance or who is by way of exemption authorized by the head of the department or his or her delegate with due regard being paid to the need- to- know principle.
- b) An authorized person shall take the prescribed oath/affirmation and complete a certificate, (Protection of Information Act 84 of 1982).
- c) Persons who must necessarily have access to classified information in the execution of their duties (the need- to -know principle) may be authorised to do so on condition that a suitable clearance has been issued or authorization has been granted, as explained above.
- d) Persons such as secretaries and personnel at smaller or remote offices or sections who in general do not have access to classified material and who do not have relevant security clearance, but are expected to have access to this information on an ad-hoc basis owing to the circumstances, will have access to such information on condition that the prescribed oath/affirmation and declaration of secrecy was completed.

- e) In terms of Promotion of Access to Information Act 2 of 2000.

10.2.6 Handling of Classified Information

a) Storage of Classified Documents:

- i) All documents will be stored in terms of National Archives Act 43 of 1996.
- ii) Classified documents that are not in immediate use must be locked away in a safe storage place, as prescribed.
- iii) The doors of all offices in which classified documents are kept must at least be fitted with security locks, and must be locked when vacated, even for a short period, by the person(s) using the room/office.
- iv) There must be proper control over access and effective control over movement within any building or part of a building in which classified information is handled.
- v) All classified documents that are dispatched, made available or distributed, must be subjected to record keeping in order to ensuring control thereof. This provision does not apply to documents that are classified as **CONFIDENTIAL**. Registers must be developed in which the particulars of classified material are to be entered.

10.2.7 Minimum Safe Storage Requirements: Classified Documents

- a) When classified documents are not in use, it must be stored in the following way:

- i) **Confidential** : Security reinforced steel cabinets,
- ii) **Secret** : Strong room, safe or security reinforced steel cabinet,
- iii) **Top Secret** : Strong room, safe or walk-in safe.

- b) The keys to any building, part of building, room, strong room, safe, steel cabinet or any other place where classified material is kept must be secured with the utmost care. An effective key control system must be established.

10.2.8 Removal of Classified Documents

- a) The removal of classified documents from office buildings is prohibited.
- b) Classified material (with the exception of **CONFIDENTIAL** documents) shall not be taken home without the written approval of the head of the department or the security manager. A list of the documents to be removed must be provided to an authorised person in control of record keeping. The "removal of classified documents" form must be completed and a copy thereof attached.

10.2.9 Typing of Classified Information

- a) Only persons having appropriate security clearance or authority from the head of the department or security manager may type classified documents. Such typing

must be done in a manner that will ensure that the information is not compromised to unauthorised persons.

- b) Drafts of classified documents, copies and floppy disks must at all times be treated as classified documents.

10.2.10 Photocopying of Classified Documents

- a) Photocopying classified /sensitive documentation is a security risk in any environment

where information of a classified nature is handled.

The following minimum requirements apply:

- i) Photocopying of classified/sensitive documents should only be allowed after approval for such copy has been obtained from the staff member entitled to give such, officially appointed by the head of department or security manager.
- ii) Photocopiers should be properly controlled to prevent the unauthorised or uncontrolled copying of classified/sensitive documents. This apparatus must preferably be centralised and under the direct control of an authorised staff member with the appropriate security grading. A central record of all reproductions of classified documents made in a particular division must be kept. For this purpose, a register is suggested which should be available at the photocopier, making provision for:
 - Date
 - Person requesting copies/reproduction
 - Classification
 - File reference
 - heading/nature of documents
 - Purpose of the copies
 - Number of copies
 - Meter reading before and after copying. (Where applicable)
- a) It is preferable that the staff member in charge of the reproduction apparatus, or an assistant entitled to do so and who has the appropriate security grading, makes these copies.
- b) In situations where copies of classified documents received from another originating authority, that is the Government Service are required, written authorisation for the copying of these documents must be obtained from the author or head of the particular division or his/her delegate(s) before copying and indicated as such on the original and the document received. (**Remark:** Authorisation could occur via facsimile and the approval should be filed with the particular document).
- c) In situations where classified documents are received from institutions other than the Government Service, it is preferred that the same procedure be followed.

However, practical considerations will normally prescribe the method to be followed and it is suggested that a clear record be kept (as mentioned earlier or written on the document concerned) of copies made and then on the principle that the head of the department or security manager must give authorisation for such duplication.

- d) Apart from recording the existence of copies in a register, a rubber stamp or red pen should be used for marking the original or file copy on the back, where the number of copies and distribution is indicated.
- e) Copies of all classified documents must be assigned a copy number and be registered in the same way as the original document. The number of copies of such documents must be restricted to a minimum and copies of appendices and addendum must be numbered in accordance with the relevant classified document. All divisions or individuals who received copies and the corresponding copy numbers must be recorded in the particular file (if applicable) or noted on the original used for copying. Alternatively, a distribution list can be attached to all copies of the document concerned, indicating the addressees and the applicable copy number. The distribution list should be filed with the copy or on the particular file (concerning the subject) and there should be a reference to the exact location of this list on the copy.
- f) Written authorization for copying of **SECRET** and/or **TOP SECRET** documents must be provided by the author, head of the department or security manager. Such authorization must be indicated on the original document.
- g) Copies of all **SECRET** and **TOP SECRET** documents must receive a copy number and be registered in the same way as the original document.

10.2.11 Sealing of Classified Documents before Dispatch

- a) Classified documents must always be dispatched in a double security plastic envelope and bag, i.e. in a security plastic envelope placed within security plastic bag. The inner security plastic envelope is stamped with the relevant classification while the external security bag is not stamped with any classification, as not to attract unnecessary attention. (documents classified as "restricted" are excluded).
- b) The security seals of the inside security envelope must be properly sealed with paper seals, counter signed on the seals and with the name of the office of origin clearly stamped on them. If paper seals are used for this purpose they must be attached with passport glue. (Seals that can be re-used are not suitable for this purpose).
- c) Thereafter wide translucent tape must be put on the seams, covering the seals and the stamps. The reference number of the document, name and address of the addressee and other special instructions for dealing with the documents must

appear clearly on the front of the inside envelope, while the security classification of the document must be indicated clearly on the front and back of the security plastic envelope by means of rubber stamp or writing in red ink.

- d) The use of **security envelopes**, designed for the purpose of securing classified information, should be used, where possible.

10.2.12 Destruction of Classified Documents

- a) In terms of the National Archives Act 43 of 1996 all documents received or created in the government service during the conduct of official affairs are subject to the Act, except where they are excluded due to their very nature or the prescriptions of some other Act of Parliament. It should be a point of departure that all state documents is subject to the Archives Act, unless justifiably excluded as mentioned above.
- b) Where destruction has been properly authorized, it should take place by burning or some other approved method, e.g. by means of a shredder (in the latter case – preferably a cross –cut machine), in which case the strips may be no wider than 1,5 mm. 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. Refer to records management policies.

10.2.13 Transmitting Classified Documents by Means of Facsimile

- a) When it is necessary to transmit documents containing classified contents by means of facsimile, only facsimile machines equipped with encryption may be used. In this regard the classified information may only be handled by staff who have a corresponding security grading, or by a member who was given authority to do so by the head of the department or security manager. Record must be kept of the transmission and receipt of all classified information sent or received through facsimile. It is also important to note that the room, in which cryptographic equipment/facsimile is kept, must be secured and locked when not in use. The recipient or the communication centre of the recipient, upon receiving the document, must ensure that it has been received clearly, accurately and in full. Thereafter, acknowledgement of receipt must immediately be transmitted to the sender, who must note the successful transmission on his/her copy of the document.
- b) Effective control must be exercised over those facsimile machines not equipped with encryption to ensure that these are not used for the transmission of classified information. However, situations may arise where the contents of classified documents must be sent over facsimiles, which are not equipped with encryption. This should be the exception rather than the rule and the following

guidelines must be followed to maintain an acceptable standard of information security:

- i) Where **Confidential or higher classified** documents are transmitted, the head of the department or security manager should give his/her approval.
- ii) The approval must be indicated on the original copy.
- iii) The recipient should be notified and, where possible, wait at the receiving facsimile to receive the document and confirm it with the sender.
- iv) The fact that the particular document was sent over an open facsimile must be indicated clearly on the original copy, including the particulars of the facsimile involved.

After receiving a message, receipt must be acknowledged immediately in the following manner:

- i) The recipient must immediately after receipt, transmit an acknowledgement of receipt to the sender.
- ii) The recipient must, on his/her copy, note the copy number, as indicated on the distribution list.

10.2.14 Securing of Classified Documents

- a) Classified documents should be secured in the most effective and appropriate way, which includes strong rooms, safes or metal cabinets, fitted with a vertical security bars and equipped with a security lock.

Important in securing classified documents, is adherence to principles stating that:

- i) Documents with classified contents that are not in immediate use must be locked away in a safe storage place as described above.
- ii) The doors of those offices in which classified documents are kept must be fitted with at least security locks and must be locked every time they are vacated by staff occupying such offices (even for a short period).
- iii) If staff leave their offices at the end of the working day, all material bearing a classification of **Confidential** or higher must be locked away in a safe or steel cabinets as described above. Apart from locking the office, staff must ensure that other possible entrances to the office, such as windows, are also closed.
- iv) It is preferred that documents bearing a **Confidential** classification be kept in a lockable filing steel cabinets and depending on its contents or the state of other security measures in the building/office, the steel cabinets should be fitted with a vertical security bar/rot and equipped with a security lock. Documents of a **Confidential** nature or higher classification should, at least, be kept in the same type of steel cabinet or, preferably, in a safe or strong room, depending on the contents and classification.

- b) Should a strong room or safe, which is equipped with a combination lock, be used for securing documents with classified contents, the combination must be changed every six months or in the following situations:
- i) When it is suspected that it has been compromised.
 - ii) If it was necessary to make the combination known to another person for whatever reason.
 - iii) When a new user takes over the safe.

Remark: A register should be used by the security division to manage the status of safes and strong rooms in a particular building. Provision should be made for recording the date when combinations are changed, the location of safes and previous users. The combination of a safe or key must be kept in a numbered and sealed security envelope at Security division and its existence could also be recorded in a register. This register is classified as **SECRET** and must be managed as such.

10.2.15 Record-Keeping of Classified Documents

- a) An important principle that must prevail when dealing with classified documents, is that a record must be kept of the manner the document is handled. This must include the entire period from the time the document is received, through the process of handling by staff allowed to have access to it, until it is finally filed, archived or destroyed. Registers must be used in this process of receiving and despatching classified documents. This regulation applies to internal communication, as well as to post received from outside organisations (including state departments), or post distributed externally.

10.2.16 Registries and Files

- a) With particular reference to the handling of classified information, the aim of a registry is to enable total control over unclassified and classified documents, including determining their temporary or permanent location. Access to registries where classified documentation is dealt with, should be strictly controlled. Only those officials attached to the specific registry or with a line-functional responsibility (provided they have the appropriate security grading) should be allowed inside the area where the files are kept. Since the classification of correspondence could only be determined once it has been opened (should it not be indicated on the envelope that contained the document) staff attached to the particular registry where all incoming mail is received should have a security clearance that corresponds with **Confidential**.
- b) Files of an official nature should be opened according to an identified need. The file reference number allocated must refer to the department's filing system and its existence should be noted in a central register that is kept in the registry

dealing with classified matters. The file should bear the same classification as that of the contents and this must be indicated at the front and back of the file. Apart from a file reference number, the subject should also be indicated on the cover of the file. (Remark. Situations could exist where the matter that is being dealt with, is sensitive. In such situations the project name, if applicable, or other similar reference, should rather be used.) Files containing classified documents should be kept in secure facilities, including the office where it is kept and access to the particular office.

- c) A sequential number marked in the right-hand corner of the first page of a document (should it contain more than one page) must be allocated to every document filed in a classified file, as indexed on a page attached to the inside of the file cover, together with the name/heading of the document concerned. In situations where an official receives a classified document in person, he/she must on returning to his/her office (for instance if that document was received while he/she was out of office) send it to the registry for recording in the relevant register. The same procedure will prevail if he/she received such document under other circumstances, such as from a visitor to his /her office.

10.2.17 Central Registries for Receiving and Dispatching Mail

- a) An effective registry is the core of effective document control and of document security. The registry should be centralised in the department where all incoming mail must be received, opened and from where it must be distributed internally. This receiving and distributing must be recorded in the relevant registers.
- b) Internal distribution should be reflected in registers.

10.2.18 Access to Main Registry

- a) Access to registries should be controlled. Any person that has no direct line functional responsibility inside the registry may not be allowed access to the area where the files are kept.

10.2.19 Management of Files

- a) Files should be opened according to the actual need when the need arises, and not just because the filing system provides for the existence of such a file.

The particulars appearing on the file should be at least:

- i. The name / topic of the file
- ii. The file number
- iii. The classification, and
- iv. Who are / is authorized to have access to that file.

- b) A register should be kept of all files opened/in existence. As and when a file is opened, the particulars must be entered in the register. This register must indicate the number of volumes in existence for any given number.
- c) A file must be classified according to the highest level of classification of the documents it contains.
- d) The classification mark must be affixed on the file as described above.
- e) All documents filed in a file must be given a serial or index number, in the sequence as it is filed, but preferably in chronological order. An index page must be fixed in the file, on which should be recorded the index/serial numbers of the documents on that file, as well as the topic /heading of each documents.
- f) A sub file must be opened for each file and kept inside the main file. It should have the same particulars as the main file. When the main file is drawn and removed from the registry (which should not be a common practice), an indication must be made on the sub file to which the main file has been issued as well as the date and time. The sub file should remain in the registry and all documents that should be filed on the main file must be placed on this until the main file has been returned.
- g) No file must be allowed to remain outside the registry for more than one working day. All files must be returned to the registry before closure on the same working day. Exceptions can be allowed, provided that storage facilities in the relevant office where the file will be kept are at the required standard (as prescribed) and that the return of the file is followed up on a daily basis by the head of the registry.
- h) Only authorised persons may be allowed access to classified files. The persons authorised with security level must also correspond with the file to be viewed/ received.

10.2.20 Sealing of Classified Documents and Courier Services

- a) Classified information in a documented form (excluding that sent by facsimile or computer) must be sealed and handled in the prescribed way to ensure that it reaches its destination unopened. Should a classified document be distributed internally, that is, to another employee in the same division or to another division, it could occur via registration in the file dealing with the subject. Files, in particular those classified as **Confidential or higher**, should be distributed in a sealed/security plastic envelope (as indicated above). Where the services of a registry clerk are used, it must be noted that the official should have a security grading that corresponds with this task on his job description. When classified documents are distributed as an independent item and where the services of a courier are used, it is important to note that a receipt must accompany all documents despatched and that this receipt must be returned to confirm receipt

of the document. (**Remark:** Receipts are cardinal in any investigation into the disappearance or mismanagement of classified information).

- b) Despatching classified documents with the aid of a courier occurs via the registry where this is recorded in the despatch register. It is preferred that the courier should convey the document(s) in a secure container or security bag or security envelope that can be locked/sealed (combination-type lock/plastic security seals/security envelopes). Couriers must identify themselves when they collect and deliver documents. Couriers, who deliver classified information, must satisfy the security clearance requirements. Classified documents should preferably not be despatched externally through commercial mail channels.
- c) **However, in cases where a courier or alternative form of delivery is not available, the use of commercial postal facilities is allowed under the following conditions:**
 - i) Must be sent by registered mail.
 - ii) The addressee must be informed that he/she will receive a classified document by registered mail and must be requested to inform the sender's registry immediately when this document is received.
 - iii) The head of the department or security manager must have given his/her express permission.
 - iv) The circumstances or reason for this decision, approval by the government official concerned and confirmation from the relevant registry official that there was no alternative, must appear on the file copy of the document that was sent.

10.2.21 Transmitting Information by Computer

- a) It is preferred that classified information sent through computerised transmission is encrypted in some or other way.
- b) A record must be kept of the classified information transmitted and received. The recipient of information having classified contents should always acknowledge receipt thereof.
- c) All magnetic media should be regarded as documents and handled as such. Classified information generated through a computer must also be supplied with copy numbers.

10.2.22 Removal of Classified Documents from Premise

- a) As a principle for sound information security, no classified information (in particular that classified as **Confidential or higher**, including electronic media containing such information) may be removed from the department where it has its origin for reasons other than despatch, unless it is absolutely essential. If required, the staff member wishing to remove such information must obtain

written permission beforehand from the employee or alternate appointed by the head of department (indicated on the persons' job descriptions) who has the authority to grant such permission. (**Remark:** The head of the department could determine, prescribe and authorise the particular manager(s) and the particular types of information, including the level of sensitive).

The written permission, of which a copy will be placed on record for future inspection (auditing) by the security division, must include:

- i) Identifying particulars of the document(s)/electronic media to be removed (file reference, date, subject/description, copy number and security classification);
 - ii) The personnel or ID number, and name of the staff member removing the information;
 - iii) The reason for removing the document(s) from the premises;
 - iv) The place/address where the information is taken to or is to be kept;
 - v) The date on which the information is to be returned; and
 - vi) The signature of the staff member removing the documents, which shall be regarded as proof that the person removing the information accepts full and personal responsibility for safeguarding the relevant information, that is, ensuring that its contents are not disclosed to unauthorised persons, organisations or institutions while in his/her possession.
- b) Information may not be taken home without the written approval of the staff member's manager or his/her delegate (as appointed by the head of the department). A list of the information to be removed must be put on record in a system designed for this purpose. Staff may take classified information home only if they have proper lock-up facilities. The manager who gives the approval for removing classified information must ensure that it is returned on the date specified. If the classified information concerned is not returned by the determined date, the issue shall be considered to constitute a breach of security and must be reported to Security division. No standing authority may be granted to remove classified information from the department's offices.
- c) It sometimes happens that a visitor or a person temporarily assigned to departments needs to remove classified information. In such situations the procedure of written permission must prevail.
- d) Where classified information is taken out of the building with a view to using this at meetings or appointments, the official utilising the information accepts full and personal responsibility to ensure that its contents is not disclosed to unauthorised persons, organisations or institutions while in his/her possession.

10.2.23 Destruction of Classified Documents

- a) In terms of the National Archives Act 43 of 1996, all documents received or created in a government office during the conduct of affairs of such office are subject to the Act, except where they are excluded, due to their very nature or the prescriptions of some or other Act of Parliament. It should be a point of departure that all state documentation is subject to the Archives Act, unless justifiably excluded along the above-mentioned lines. It should be noted that no document is to be excluded merely because it is classified. The heads of department will have to decide, after consultation with their legal advisers 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.
- b) Where destruction has been properly authorised, it should take place by **burning** (incinerator) or some other approved method, e.g. by means of a **shredder** (in the latter case - preferably a cross-cut machine), in which case the strips may be no wider than 1, 5 mm. The officer who has destroyed the documents must give a certificate of destruction of the documents concerned to the head of the department or his delegate.
- c) The process of destruction must be such that reconstitution of the documents destroyed is impossible.
- d) If the necessary precautions are not instituted, access to waste-paper baskets is probably one of the easiest ways for unauthorised persons to obtain sensitive information. Special attention should therefore be given by all those concerned to the disposal of drafts, notes, used carbon paper, typewriter ribbons, etc., that may contain information. Such waste must be stored separately under lock and key and must be periodically collected by an officer(s) specially designated for this purpose and destroyed by means of burning or shredding.
- e) In terms of the procedure for the destruction of classified documents from other departments /institutions, a destruction certificate must be supplied to the author of the document.
- f) Classified information (documentation) which is not needed anymore, for instance drafts, or which has become redundant, must be destroyed properly by means of a burning (incinerator) or shredder. It is preferred that the originator of the (classified) document, or the staff member who has used this information, depending on its sensitivity, destroys it him/herself. Electronic media on diskettes could be destroyed through incinerating or rewriting over the existing data, using a particular program for that purpose, allowing unintelligible characters to write over the data, or through introducing the contents of the diskette to a magnetic field, which will erase the contents. Depending on the level of sensitivity of drafts, control must also be exercised over their destruction. It is important to note that

a regulation exists which stipulates that a declaration (destruction certificate) must be made out (in writing) when original official classified documents are destroyed and that the originator must be informed of this.

10.2.24 Meetings

- a) When the intention is that documents that contain classified information are to be removed from the office / building to a venue where a meeting will take place, the particular staff member must ensure that prior to the distribution of the classified information at the meeting:
 - i) The recipients of the documents are in possession of the appropriate security grading, that is, that the outcome of the particular person's integrity assessment corresponds with the sensitivity of the information to be distributed, or that the recipient obtained approval beforehand from executive level to do so;
 - ii) The recipients of the documents have a secure means of carrying and transporting the information to their offices;
 - iii) The information concerned has been recorded in the register for outgoing documents; and
 - Each recipient is issued with a letter of authority, permitting him/her to remove the documents from the division after he/she has signed for receiving them.
 - The officials attending the meeting should further complete a "Protection of Information Certificate".

10.2.25 Security Inspection of Files Containing Classified Documents and Registers Referring to the Position of Such Information

- a) To ensure that documents containing classified information in possession of the department are dealt with in the prescribed manner, Security division must on an annual regular basis undertake information security inspections (audits) of all official corporate files containing classified documents. Inspection of all registers used by the divisions for recording the receipt and despatch of classified information, as well as records of photocopies made and facsimiles sent, or records kept on the movement of classified information such as removal of classified documents from any government premises, must be carried out.

10.2.26 Handling of Classified Information in Emergency Situations

- a) The contingency plan of a division must provide for the destruction, storage and/or moving of classified information in the event of an emergency, in order to prevent the risk of being compromised.

10.2.27 Loss of Classified Information

- a) Should classified documents be lost or mislaid, this must immediately be reported in writing to the Security division. An investigation in consultation with the head of department must be instituted and appropriate, corrective steps taken. Such corrective steps may include disciplinary actions.

10.2.28 Security Marking of Documents

- a) Physically marking classified information with appropriate classification and control markings serves to warn and inform holders of the degree of protection required.

10.2.29 Documents and Bound Volumes

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

10.2.30 Copies, Tracings, Photographs, Drawings, Sketches

- a) Security classifications should be indicated on such copies, photographs, sketches, etc., by means of rubber stamps or writing in red ink. The exact position of the mark may vary, depending on the nature of the document, so that the stamp/writing do 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. 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/writing in red ink should be used to mark all the copies. Care should be taken not to damage the document's authenticity with the security marking thereof.

10.2.31 Rolled or Folded Documents

- a) Apart from being marked as prescribed on the face, a document such as this should also be marked in such a way that the security classification will be clearly visible when the document is folded or rolled up.

10.2.32 Tape Recordings and Documents on Which No Marks Can Be Made

- a) Where, as in the case of tape recordings, certain photographs and negatives, it is physically impossible to place clear classification marks on a document 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.

10.2.33 Contingency Planning: Document Security

- a) The contingency plan of the department must provide for the destruction, storage, protection and/or removal of classified/sensitive documents in the event of an emergency, to prevent the compromise thereof.

10.2.34 Reporting of Incidents which may Influence a Person's Security Competence

- a) Departmental officials must report all aspects or incidents which may adversely influence the security competence of an employee or any other person, executing duties in the department, to Security Manager regardless of the security clearance level of the person involved. The following aspects, which may have an influence on a person's security competence, must be reported:
- i. Any action, negligence or behaviour that exposes classified information, plans, human resources, infrastructure, installations or equipment to any exploitation that may be detrimental to the security of the Provincial and National Government.
 - ii. Radicalism that manifests itself in fanatical behaviour, acts of violence or terror, murder, intimidation or intimidating behaviour.
 - iii. Addiction to alcohol, drugs, medicine or other addictive substances (including dagga but excluding tobacco). The frequent use of addictive substances, drugs or medicines (including dagga but excluding tobacco), which indicates a continued pattern of misuse.
 - iv. Involvement in dealing with or the supply of illegal drugs.
 - v. A continued pattern of serious alcohol abuse.
 - vi. Multiple relapses after treatment for alcohol abuse, drug abuse (including dagga) or the abuse of other addictive substances (excluding tobacco).
 - vii. Financial difficulties leading to multiple summonses for debt, the administration of his/her estate, sequestration or the repeated borrowing of money and failure to repay creditors.
 - viii. Repeated lapses into financial difficulties indicative of a person's inability to manage his/her personal finances.
 - ix. Involvement in fraud, corruption, theft or any criminal activities, criminal investigation by the South African Police Service as well as any criminal convictions.
 - x. Any civil offence (excluding traffic violations).
- b) It must be emphasised that the above-mentioned aspects judged individually, in combination with one another or in combination with other aspects, may have an influence or bearing on a person's security competence.

- c) All reports relating to security breaches or failure to comply with security measures, or conduct constituting a security risk should be reported to the office of the security manager. Where appropriate and depending on the nature of the security breach, the incident may be communicated to the State Security Agency (SSA), South African Police Service (SAPS) or South African Communication Security Agency (SACSA).

10.3 PERSONNEL SECURITY

10.3.1 Personal Suitability Checks

- a) Criteria for personnel suitability checks (PSC is valid for a year). The following will be scrutinised when the candidate is to be employed in the organ of state, in terms of National Vetting Strategy of 2006 issued to supplement the Public Service Regulation 2001, Chapter 1 part VII D.8(a) that deals with the verification of candidates' information prior to appointment/filling of a post:
 - i. Criminal records checks,
 - ii. Citizenship status verification,
 - iii. Credit worthiness checks,
 - iv. Qualification verifications.
- b) After a month the candidates has been appointed full security vetting will be conducted through State Security Agency (SSA).
- c) Security vetting is the systematic process of investigation followed in determining an official's security competence.
- d) The degree of security clearance given to an official is determined by the content of and/or access to classified information entailed by the post already occupied/to be occupied by the official.
- e) 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 official's vulnerability to blackmail or bribery or subversion and his/her loyalty to the state or the department do. This also includes compromising behaviour.
- f) A clearance issued in respect of an official is merely an indication of how the person can be utilised, and does not confer any rights on such an official.
- g) A declaration of secrecy in accordance with the Protection of Information Act, 82 of 1984. **A Z204 security clearance questionnaire** must be completed on the official form, by each and every departmental official and applicant for a post that has access to classified information, before he/she is appointed or during the appointing process.

- h) All other officials and any other individual from the lowest level up to deputy director-general, who should have access to classified information, must be subjected to security vetting.
- i) A security clearance gives access to classified information in accordance with the level of security clearance, subject to the need-to-know principle.

10.3.2 Vetting Criteria

- a) Vetting/screening criteria needs to be adjusted continuously owing to the development in the political field and changes in the social and socio-economic fields. On a macro level, screening criteria must be adjusted to the norms and values of the community of which the person is a part. However, on the micro level, screening criteria must provide for the unique nature of individuals and the department. The overall picture of individual differences and the individual's unique way of handling situations has to play a determining role in a vetting recommendation or decision.

10.3.3 Security screening in respect of immigrants and officials with more than one citizenship

a) Confidential Clearance

A confidential clearance may be considered in respect of an immigrant who has been resident in the RSA for five consecutive years, and is a South African citizen. He/she must provide sufficient proof that any former citizenship has been relinquished.

b) Secret Clearance

A secret clearance is only considered in respect of an immigrant who has been resident in the RSA for fifteen consecutive years of which at least those ten years preceding the clearance were spent as a South African citizen, also on the condition that the person has relinquished his former citizenship.

c) Top Secret Clearance

After an immigrant has been resident in the RSA for a period of twenty consecutive years (of which fifteen years were spent as a South African citizen), a top-secret clearance may be considered, on condition that such a person has relinquished his former citizenship. Every case will be dealt with on merit owing to the unique nature of each situation. This means that not all immigrants who comply with the requirements will automatically qualify for a top-secret clearance.

d) Dual Citizenship

Each application for a security clearance in respect of persons with dual citizenship must be assessed on the merits of each individual case.

Persons Without Valid Identification Documents

No clearance can be issued in the following cases:

- Any person who is not in possession of a valid identification document or residence permit for the RSA.
- Naturalised RSA citizens who have not applied for a new identification document after naturalisation, since the document that was issued before naturalisation, expires on naturalisation.

Employing Immigrants Who Do Not Meet Clearance Requirements

If on account of his/her indispensable expertise, it is considered essential to employ an immigrant while he/she does not satisfy the clearance requirements as laid out above and he/she is to be utilised in a post, the work of which is classified, the vetting authority will be unable to make a positive recommendation with regard to the issue of a security clearance in respect of such a person, but can merely institute an investigation to determine whether such an immigrant is suitable from a security point of view for the post concerned. In such an event the head of the department may authorise that the immigrant be used in the post on the condition that the employing institution must;

i) Submit a certificate to the State Security Agency and the responsible screening institution in which the absolute necessity of employing such immigrant is set forth and it is also declared that no RSA citizen with the same expertise is available or can be recruited in the RSA and, in cases where an immigrant from a state formerly seen as controversial has been employed, that an immigrant from a non-controversial country could not be obtained;

- i) Provide the responsible screening institution with a description of and an indication of the sensitivity of the responsibilities attached to the post to be occupied by the immigrant;
- ii) Declare that he/she accepts full responsibility for compliance with the security requirements connected with the employment of such immigrant;
- iii) Ensure that no classified information or material that is not needed for the performance of his/her duties comes into the possession of the incumbent of the post; and
- iv) Reconsider the authorisation every year and relate in writing to both the State Security Agency and the responsible screening authority any incident which could pose a threat to security or any incidences which may bring his/her security competence into question.
- v) **Note:** When the person concerned changes his/her posting, the authorisation is automatically terminated.
- vi) In respect of immigrants already employed in sensitive positions and in whose case the conditions laid out as above have not yet been complied with, the employing institution must immediately give effect to those conditions.

10.3.4 Screening of officials who have lived/worked abroad for long periods

- a) Where a security clearance is required for an RSA citizen who has resided/studied/worked abroad for a long period (excluding transferred public servants or students) and who applies for a position in the department, such a person is temporarily not eligible for any grade of security clearance. Applications for security clearance can, however, be considered after a period, as set out hereunder, on condition that the applicant did not give up RSA citizenship or accepted dual citizenship during the period of absence.
- b) A confidential clearance after one year back in the RSA. Such a person can be appointed on condition that a re-application is submitted after one year. On appointment, the subject thus completes and submits all relevant forms for a security clearance. The requesting authority will then be informed as to whether or not there is any negative information on the subject. The subject is also to undertake, in writing, that he/she will resign should the issuing of a security clearance be refused after one year. If such an undertaking is not specifically included in the service contract, a written undertaking to this extent, under signature of the subject, must accompany the application for a security clearance.
- c) A secret clearance after three years back in the RSA.
- d) A top secret clearance after five years back in the RSA.

10.3.5 Security Screenings of Contractors Supplying Services to the Department

- a) As the onus is on the department to indicate expressly in documents sent to the state tender board or private contractors what the security implications that should be taken into account in advance are when they perform their duties for the department. As the department is in possession of sensitive information there are possible implications of the information being compromised. A reason must be given for the inclusion of a clause in the tender document indicating the degree of clearance required, as well as a clause to ensure the maintenance of security during the performance of the contract. The clause could read as follows:
“Acceptance of this tender is subject to the condition that both the contracting firm and its personnel providing the service must be cleared by the appropriate authorities to the level of CONFIDENTIAL / SECRET / TOP SECRET”.
- b) The obtaining of a positive recommendation is the responsibility of the contracting firm concerned. If the principal contractor appoints a subcontractor, the same provisions and measures will apply to the subcontractor.

- c) Acceptance of the tender is also subject to the condition that the contractor will implement all such security measures as the safe performance of the contract may require.”
- d) The department must determine the security responsibilities of the contractor and the security manager must be involved to advise directorates in this regard.

10.3.6 Period of Validity of Security Clearances

- a) The head of department or his/her delegate must ensure that an officer in respect of whom a security clearance of secret or top secret has been issued, is re-screened every five (5) years and every ten years in respect of a confidential clearance.
- b) Enquiries will be done with the supervisor every five (5) years with respect to the security competence of an official who has received a confidential clearance.
- c) This arrangement does not preclude re-screening before a period of five years has lapsed in the case of occupational change or where something prejudicial has been established about an officer which may affect his or her security competence. Personnel in ultra-sensitive posts should be cleared every three years.

10.3.7 Transferability of Security Clearances

- a) A security clearance issued in respect of an officer while he/she is attached to a particular institution is not automatically transferable to another institution, for example when the officer is transferred. When an officer changes his employer, the responsibility for deciding whether an applicant's existing clearance will be accepted or whether the re-screening of such an officer will be requested in the prescribed way rests with the new employer. The previous vetting clearance status of the transferred official could therefore be considered by security division. Depending on the security level and period of validity of the existing vetting certificate and responsibilities of the new post, the official may be subjected to a new vetting investigation.
- b) However, for the purpose of meetings and other co-operative functions clearances are transferable. The employing institution is responsible for informing the chairman of such a meeting in writing as to the level and period of validity of the clearances of the representatives involved.

10.3.8 Responsibilities of the Screening Authority

- a) The screening authority will investigate and advise on the security competence of a person on the basis of prescribed guidelines.
- b) After the investigation the screening authority will merely make a recommendation regarding the security competence of the person concerned to

the head of department, and this should in no way be seen as a final testimonial as far as the utilisation of the person is concerned.

10.3.9 Responsibilities of the Head of the Department with regards to Security Clearances

- a) The head of the department or security manager must make a decision and issue a clearance after receiving the recommendation made by the screening institution, and in accordance with circumstances/information at his/her disposal.
- b) Notwithstanding a negative recommendation from the screening authority, for whatever reason, the head of the department may still, after careful consideration of recommendations by the security manager, and with full responsibility, use the person concerned in a post where he/she has access to classified matters if she is of the opinion that the use of the person is essential in the interest of the RSA and her institution, on the understanding that a person satisfying the clearance requirements is not available.
- c) When **any** such a person is utilised without a clearance, the State Security Agency must be furnished every year with a certificate regarding such person's security conduct. Any conduct entailing a security risk must be reported immediately to the office of the security manager, for coordination with the screening authority concerned.
- d) The head of the department, security manager or head of branches, as the case may be, whose officials attend meetings where classified matters are discussed must inform the chairperson of such a meeting in writing of the level of security clearance of such officers. It is the responsibility of the chairperson to satisfy himself/herself regarding the security clearance of all those present at the meeting.
- e) Further, it is also the responsibility of the heads of branches:
 - i) To ensure that there is continuous supervision of persons in respect of whom security clearances have been issued.
 - ii) Caution staff members not to supply personal particulars of colleagues/officials to unauthorised persons.
 - iii) Ensure that persons dealing with classified matters sign the prescribed declaration of secrecy and complete the security vetting questionnaire (Z 204).
 - iv) Pertinently bring to the attention of the officials working with classified matters any other legislation, regulation and/or orders that entail secrecy and/or the protection of activities, installations, etc., of the department.
 - v) To point out to employees dealing with classified matters when they resign or leave the service that they will continue to be the target of foreign

intelligence services and that they remain subject to the declaration of secrecy, which is renewable every five years.

- vi) To ensure that all classified documents in the possession of the person concerned are returned when such person resigns or leaves the service; and.
- vii) To ensure that no information comes into the possession of an individual that is not essential for the performance of his or her duties. (need-to-know principle).
- viii) Request assistance from Security division on any matter related to the above or security policy.

10.3.10 Responsibilities of Officials Travelling Abroad on State Missions

- a) In the event where an official travel abroad, the head of the divisions must inform the office of the security manager of such a visit for a security awareness briefing. A thorough record must be kept of these visits.
- b) Officials travelling abroad must be on their guard against any attempt by a foreign intelligence service or crime syndicates to recruit them. If a person is approached, he or she must, immediately on returning, report the fact to the security manager. While travelling, officials should maintain a low profile and be careful not to place themselves in compromising situations.
- c) Officials travelling abroad are required to complete a classified questionnaire, which will be provided by security division, and be updated from time to time. The information is for emergency situations while abroad.

10.4 COMMUNICATION SECURITY

- a) No Encryption devices shall be allowed except those approved by and COMSEC and/or any other approved institution.
- b) Communication devices include fax machines, telephones, cell phone, computer, laptops/notebooks and any other electronic devices used to convey information from one person to another.
- c) Access to communication security equipment of the department and the handling of information transmitted and/or received by such equipment, shall be restricted to authorised personnel only.
- d) All facsimile machines used to send and receive classified/sensitive documents must be encrypted as prescribed. An SFU 1000 (Secure fax Unit) must be installed on all fax machines used to fax classified documents. When a classified document is faxed the sender must ensure that the fax machine of the receiver is also equipped with the same equipment.
- e) A register for all classified faxes must be kept separate from the normal fax register. The register must also be classified to the same classification of the highest classified document indicated in the relevant register.

- f) The same rule applies to telephones and cellular phones. Telephones used by MEC, HoD, and strategic offices must be equipped with the requires scrambling equipment (SSU 600).
- g) Computers and servers must be equipped with the latest firewalls and encryption software as well as the latest antivirus software to prevent unauthorised access through internet and intranet connections as well as the malicious damage caused to the system by viruses and Trojan horses.

10.5 TECHNICAL SURVEILLANCE COUNTER MEASURES (TSCM)

- a) All offices, meeting, conferences and boardroom venue of the Department where sensitive and classified matter are discussed on a regular basis shall be identified and shall be subjected to proper and effective physical security and access control measures. Periodic electronic Technical Surveillance Counter Measures (sweeping) will be conducted by State Security Agency to ensure that these areas are kept sterile and secure.
- b) The security Manager shall ensure that areas that are utilised for discussions of a sensitive nature as well as offices or rooms that house electronic communications equipment, are physical secured in accordance with the standards laid down by State Security Agency in order to support the sterility of the environment after a TSCM examination, before any request for TSCM examination is submitted.
- c) No unauthorised electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of the department of Limpopo Provincial Treasury is discussed. Authorisation must be obtained from the Security Manager.

10.6 INFORMATION SECURITY

10.6.1 Responsible Use: Ethics in Computer Usage

- a) Everyone within the department who uses departmental computing and communications facilities has the responsibility to use them in an ethical, professional and legal manner. This means that users agree to abide by the following conditions:
 - i) The integrity of the systems must be respected. This means that users of systems will not divulge passwords, pins, private keys or similar elements to anyone else, and they will not exploit sessions left open or otherwise misappropriate or steal the "identity" of another user.
 - ii) Privacy of other users must not be intruded upon at any time.
 - iii) Users must recognize that certain data are confidential and must limit their access to such data to uses in direct performance of their duties.

- iv) The rules and regulations governing the use of facilities and equipment must be respected. Persons responsible for computing devices connected to the network will ensure that those devices are maintained in a secure state in accord with related **IT POLICY**.
- v) No one shall obtain unauthorized access to other users' accounts and files.
- vi) The intended use of all accounts, typically for organization, instruction and administrative purposes, must be respected.
- vii) Commercial use is prohibited.
- viii) Users shall become familiar with and abide by the guidelines for appropriate usage for the systems and networks that they access.

10.6.2 Measures to be implemented

- a. Essential backup of computer systems and data;
 - i. Physical security measures as prescribed;
 - ii. Computer security responsibilities should be clearly established;
 - iii. The allocation and use of passwords as prescribed on all sensitive and classified documents, including e-mail.
- b) Where use is made of computer communications and data is transmitted through an unprotected area, the transmission should be protected in accordance with communication security policy/Instructions.
- c) All breaches of security in the computer environment must be reported as soon as possible in accordance with this document to the office of the security manager.
- d) In cases of uncertainty regarding the implementation or appropriateness of security measures in the computer environment, the office of the security manager must be approached for advice.

10.7 CRYPTOGRAPHIC SECURITY

10.7.1 Cryptography

It is the conversion of data into a secret code for transmission over a public network, in order to preserve information security such as data confidentiality, data integrity, and authentication.

10.7.2 Cryptographic Security Compromise / Violation

Cryptographic security compromise or violation occurs whenever unauthorised persons gain knowledge or intercept messages and /or material and equipment related to the crypto environment.

10.7.3 Chief Communications Officer

- a) A chief communications officer must be appointed to manage cryptographic security in the department. The head of information technology security, security division, shall assume these responsibilities and functions.
- b) The chief communications officer must maintain a classified register of all communication security equipment issued to the department. Receipt vouchers, signed by the authorized recipients, are to be returned to COMSEC without delay and all controlled equipment are to be accounted for until it has been withdrawn.
- c) The application of preventative cryptographic security measures is the responsibility of each official who has been authorised to access crypto documents and information thereto.

10.7.4 Clearance of Personnel Utilising/Managing Cryptographic Equipment

- a) Only RSA citizens, who do not have dual citizenship, in possession of a security clearance of "secret" may have access to or utilise cryptographic equipment.
- b) Officials operating crypto equipment must have a security clearance of **SECRET**.
- c) Contrary to other security clearances, the validity of a security clearance issued to a cryptographic custodian, is three years.

10.7.5 Cryptographic Custodians

A primary and secondary (alternative) custodian must be appointed in writing for each office where cryptographic equipment is deployed.

10.7.6 Responsibilities of Primary and Secondary Custodians

- a) Receipt, accounting and safe custody of all crypto material, registers and equipment under their control.
- b) The secure management of all crypto material, registers, equipment in accordance with COMSEC and departmental policies, regulations and procedures.
- c) Immediately report any security breach / violation to the security manager.
- d) The secure management of keys to the office / area where the crypto equipment is deployed / installed.
- e) The primary custodian must ensure that a handing-over certificate is completed each time the responsibility is taken over by the secondary custodian, due to absence for prolonged periods.
- f) Ensure that all registers and files are kept under lock and key at all times, when not in use.
- g) The secondary custodian takes over all the responsibilities whenever the primary custodian is absent.

10.7.7 Maintenance of Cryptographic Equipment

- a) The repair and / or maintenance of crypto equipment may only to be done by the COMSEC.
- b) No person, including officials reporting to be from COMSEC, may be allowed to maintain / check /repair / remove / replace any cryptographic equipment without the approval of the security manager. The credentials of any person (including officials from COMSEC) requesting access to the cryptographic equipment must be thoroughly checked and verified, **prior** to any access provided. The verification of such persons and official status will in all cases be provided by the office of the security manager.
- c) **Any** repair or maintenance to **any** telephone lines, air conditioners, electricity or other maintenance in offices where cryptographic equipment is held, must be reported to Security division, for verification, prior to any services being provided.

10.7.8 Compromises and Violations

Any official having knowledge of, or suspecting that communication security material/equipment has been lost at any stage or has been compromised or that any information pertaining thereto has become known to unauthorized persons, must immediately report such information to security manager. The circumstances shall be investigated and reported to COMSEC.

11. DEVIATION

Any policy, procedure, or guideline that does not follow the procedures and processes outlined in this policy will not be approved by the relevant authority.

Any employee who contravenes the provisions of this policy which may lead to violations of the Public Service Code of Conduct or any rules or policies, that employee shall be charged with misconduct and the necessary disciplinary measures will be taken against him or her.

12. COMMENCEMENT DATE

The commencement date of this policy will be on the date of its approval.

13. REVIEW AND UP DATE PROCESS CONDITIONS

This policy will be reviewed by the department **after two years** or when necessary. The amendments resulting from the review will be processed in line with the departmental policy development framework. However, where it is deemed not necessary to review the policy, evidence of the process leading to such decision should be provided.

This policy will remain in force until and unless it has been withdrawn or amended by Executive Authority.

14. ENQUIRIES

Enquiries regarding this policy should, in the first instance, be directed to the security manager.

15. RECOMMENDATION AND APPROVAL

Recommended for approval by:

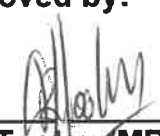


G Pratt
Head of Department

28/7/2017

Date

Approved by:



Rob Tooley (MPL)
Member of the Executive Council

21/07/2017

Date