



SECURITY POLICY

ABBREVIATIONS USED IN THIS DOCUMENT

OH&S	:	Occupational Health & Safety Act
MFMA	:	Municipal Finance Management Act
PSIRA	:	Private Security Industry Regulation Act
MISS	:	Minimum Security Standards.
MEXCO	:	Management Executive Committee
NIA	:	National Intelligence Agency
SABS	:	South African bureau of Standards
SMF	:	Security Managers Forum
SACSA	:	South African Communication Security Agency
DMS	:	Document Management System
MEC	:	Member of Executive Council

The policy deals with the broader issues of security. In some parts of the policy, reference is made to procedures which individual departments will need to develop to suit their particular environments. Heads of Departments therefore have a responsibility of ensuring that such procedures are developed.

This policy has been based on the national security policy (Minimum Information Security Standards).

In order to determine the extent to which departments implement this policy, security appraisals will be conducted on a yearly basis with the help of NIA and the relevant structures within the SAPS.

TABLE OF CONTENTS

<u>Chapter 1</u>		Page
1.1	Vision	5
1.2	Mission	5
<u>Chapter 2</u>		
2.1	List of Applicable Acts and Directives	6
2.2	Definition of applicable Acts and Directives	7
<u>Chapter 3</u>		
3.1	Obligations and Responsibilities by Stature	12
3.2	Allocated Responsibilities	12
3.3	Statutory Responsibility	13
3.4	Administration Responsibility	13
3.5	Functional Responsibility	13
3.5.2	The Roles and Function of the Security Manager	13
3.5.3	The Roles and Functions of the Departmental Security Administration Components	15
3.5.4	The Duties of Security Officers	15
3.5.5	The Duties/Functions of Security Administration Components	16
3.5.6	The Roles of Security Managers in Provincial Government	16
3.5.7	The Roles and Functions of the Provincial Security Committee	18
<u>Chapter 4</u>		
	Document Security	20
<u>Chapter 5</u>		
5.1	Personnel Security: Guideline with respect to Security Vetting	42
5.2	Security Awareness	52
<u>Chapter 6</u>		
	Communication Security	53
6.1	Categories of Communication	53
6.2	Transmitting the Classified Information	53
6.3	Personal Communication of Sensitive or Classified Information	53
6.4	The Advise/Services of NIA or SACSA on Communication Security Needs	54
6.5	Communication to the Media	
<u>Chapter 7</u>		
	Computer Security	55

Chapter 8

Physical Security	57
8.1 General	57
8.3 Access Control	58
8.4 patrol	60
8.5 Key Control	61
8.6 High Risk Areas within Buildings	61
8.7 Prescriptions in Respect of Firearms	62
8.8 Security Contracts with Private Security Contractors	62
8.8.1.3 Needs Assessments	62
8.8.2 Request for Tenders	62
8.9 Guarding and Training	63
8.16 Office Security	65
8.17 Open Plan Offices	66
8.18 Smoking in Municipal Buildings	67
8.19 Personal Belongings	67
8.20 Parking	68
8.21 Contingency Planning	68
8.22 Breaches of Security	69
Bibliography	91

CHAPTER 1

1.1 **Vision**

The Endumeni Municipality strives to provide a safe and security working environment conducive for efficient and uncompromised delivery of services.

1.2 **Mission**

The mission of Endumeni Municipality is to protect persons in the working environment, assets and information belonging to and under the care of the municipal government, through the development and implementation of:

- A Security Policy
- Security measures
- VIP Services
- Security and investigation capability
- Security training
- Loss control measures
- Occupational Health & Safety Act

This document serves as the Municipal Policy in respect of security related matters and must be dealt with as such.

CHAPTER 2

LIST OF APPLICABLE ACTS AND DIRECTIVES

2.1 The following acts and amendments support the contents of this policy and empower the introduction of security measures at Endumeni Municipality sites and institutions.

2.1.1 Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985) along with Government Gazette Notice 1042 of 6 October 1986 and 1094 of 24 May 1991

2.1.2 The Criminal Procedure Act, 1977 (Act 51 of 1977) as amended

2.1.3 The Protection of Information Act, 1982 (Act 84 of 1982) as amended

- 2.1.4 The Occupational Health and Safety Act, 1993 (Act 85 of 1993) as amended
- 2.1.5 The Trespassing Act, 1959 (Act 6 of 1959)
- 2.1.6 The Weapons and Ammunition Act, 1993 (Act 75 of 1969) (as amended)
- 2.1.7 Promotion of Access to Information Act (Act 2 of 2000)
- 2.1.8 National Archives of South Africa Act (Act 43 of 1996)
- 2.1.9 The National Strategic Intelligence Act
- 2.1.10 Municipal Finance Management Act, 2003 (Act 56 of 2003)
- 2.1.11 The Public Services Act, along with the relevant Regulations and Codes as amended
- 2.1.12 Minimum Information Security Standards
- 2.1.13 RSA Constitution Act 108 of 1996
- 2.1.14 Fire Brigade Act, 1987 (Act 99 of 1987)
- 2.1.15 Hazardous Substance Act, 1973 (Act 15 of 1973)
- 2.1.16 Labour Relations Act, 1995 (Act 66 of 1995)
- 2.1.17 National Building Regulations and Building Standards Acts, 1977 (Act 103 of 1977)
- 2.1.18 Radio Amendment Act, 1991 (Act 99 of 1991)
- 2.1.19 telecommunications Act, 1996 (Act 103 of 1996)
- 2.1.20 Tobacco Products Control Act, 1993 (Act No. 83 of 1993) as amended by the Tobacco Products Control Amendment Act, 1999
- 2.1.21 Arms and ammunition Act, 1969 (Act 97 of 1969)
- 2.1.22 The Protection of Disclosures Act 2000
- 2.1.23 Private Security Industry Regulation Act, 2000 (Act 56 of 2000)
- 2.1.24 Treasury Regulations for Department, Constitutional Institutions and Trading Entities (Government Gazette No. 21249, published on 31 May 2000)

2.2

Definition of applicable Acts and Directives

2.2.1 Arms and Ammunition Act 1969 (Act 97 of 1969)

The Endumeni Municipality is the licence holder of a number of firearms and therefore has to adhere to the Act in respect of the control, issue and safeguarding of the firearms.

2.2.2 The Republic of the RSA Constitution Act, 1996 (Act 108 of 1996)

The security personnel in executing their duties as promulgated in the legislation, may not infringe on the individual's right.

2.2.3 Control of Access to Public Premises and Vehicle Act, 1985 (Act 53 of 1985)

This security personnel have been authorized to act on behalf of the owners of the premises in terms of Section 2(2)(g) of the Act as promulgated in the Government Gazette, 20 July 1990 (No. 1264&, Notice No. 1631 and Government Gazette, 19 July 1990 (No. 13416) Notice No. 1648.

2.2.4 Criminal Procedure Act 1977 (Act 51 of 1977)

The following sections in the Criminal Procedure Act are applicable to security officers while conducting their duties:

2.2.4.1 Section 20 Municipality may seize articles

2.2.4.2 Section 23 Search of arrested persons and seizure of articles

2.2.4.3 Section 24 Search of premises

2.2.4.4 Section 27 Resistance against entry or search

2.2.4.5 Section 29 Search to be conducted in decent and orderly manner

2.2.4.6 Section 39 manner and effect of arrest

2.2.4.7 Section 40 Arrest of private person without warrant

2.2.4.8 Section 48 Breaking open premises for purposes of arrest

2.2.4.9 Section 49 use of force in effecting arrest

2.2.5 Fire Brigade Act, 1987 (Act 99 of 1987)

This Act is applicable in respect of Departments which needs to comply to Regulations and Notices issued under this Act for the safety of the community which includes personnel and public.

2.2.6 Hazardous Substances Act, 1973 (Act 15 of 1973)

This Act regulates the licensing, use and safety of “x-ray equipment” as well as personnel and public’s personal safety to exposure, including the training of operators when the equipments are used in the premises of the Endumeni Municipality for the searching of persons in access control points.

2.2.7 Labour Relations Act, 1995 (Act 66 of 1995)

This Act call for the “consultation and joint decision making” with the implementation of the policy to ensure all agree to the policy. Minimum information Security Standards (MISS) policy document, (as approved in Cabinet on 4 December 1996)

2.2.8 National Archives Act, 1996 (Act 43 of 1996)

This Act is applicable with regards to the safeguarding and disposal of documents. This Act also address access or non-access to such documents under certain circumstances.

2.2.9 National building Regulations and Buildings Standards Acts, 1977 (Act of 103 of 1977)

The National building Regulations and especially the SABS 0400 contains all the applications to ensure that the safety standards are followed in the construction or upgrading of buildings.

2.2.10 Occupational Health and Safety Act, 1993 (Act 85 of 1993)

The OH&S Act stipulates the responsibilities of the employer to provide a safe and security environment for the employees. Further, the Act stipulates the responsibilities of employees to ensure that they adhere to the rules laid down by the employer to provide a safe working environment.

2.2.11 Promotion of Access to Information Act, 2000 (Act 2 of 2000)

This Act addresses the steps to be taken by the Departments in providing information requested by certain individuals or bodies, etc. And also what need not to be disclosed.

2.2.12 Protection of Information Act, 1982 (Act 84 of 1982)

The Protection of Information Act addresses the consequences of persons who have access to sensitive information and who intentionally and unintentionally divulging it to unauthorized persons.

2.2.13 Municipal finance Management Act 2003 (Act 56 of 2003)

The MFM Act covers the responsibility, control measures, etc, of Local Government employees to minimize and control the unlawful, irregular expenditure, etc. This includes Asset Management.

2.2.14 Radio Amendment Act, 1991 (Act 99 of 1991)

This Act regulates the licencing of radio frequencies and as the Municipality has radio networks for security personnel communication via two-way radios this Act is applicable.

2.2.15 Private Security Industry Regulation Act, 2001 (Act 56 of 2001)

This is applicable to all departments employing in-house or private security personnel/companies. This is to enable the security industry to comply with the PSIRA regulation and code of conduct.

2.2.16 Telecommunications Act, 1996 (Act 103 of 1996)

The Act addresses the radio licences, frequencies, radio procedures and applies to all departments employing security officers.

2.2.17 The Trespass Act, 1959 (Act 6 of 1959)

The Act addresses the procedures and action to be taken against persons who unlawfully obtain access to a premises.

2.2.18 Treasury Regulations for Departments, Constitutional Institutions and Trading Entities (Government Gazette No. 21249 published on 31 May 2000)

These regulations need to be compiled to in respect of a number of aspects which will be covered in the policy of which, Internal Control, Asset Management, Investigations, etc., are a few.

2.2.19 Tobacco Products Control Act, 1993 (Act No. 83 of 1993) as amended by the Tobacco Products Control Amendment Act, 1999 (Act 12 of 1999)

This Act stipulates where and under what conditions is smoking permissible.

2.2.20 The Weapons and Ammunition Act, 1969 (Act 75 of 1969)

2.2.21 The National Strategic Intelligence Act

2.2.22 The Public Services Act

2.2.23 The Protection of Disclosures Act, 2000

NOTE: In applying all of the abovementioned security measures, the security officers are protected by Section 36(1) ("limitation of rights") of the Bill of Rights Act, 1996 (Act 108 of 1996)

CHAPTER 3

OBLIGATIONS AND RESPONSIBILITIES BY STATUTE

3.1 A number of organizations have been appointed custodians of certain specific security functions and responsibilities at national level. These organizations have been designated the duty of creating guidelines, giving advice and enforcing policies and procedure throughout Government Departments, Parastatals, National Key Points, etc.

3.2 The Responsibilities are allocated as follows

3.2.1	Technical Surveillance Counter Measures (TSCM)	NIA
3.2.2	Personal Security	NIA iro Vetting
3.2.3	Information Technology (Computer and Communication Security	NIA
3.2.4	Document Security	NIA
3.2.5	Information Security	NIA
3.2.6	Communication Security (Telephone & fax media, computers)	SACSA
3.2.7	Physical Security	SAPS VIP Protection Unit iro Mayoral & MEC's homes and offices. SAPS Security Advisory Services iro all other physical security
3.2.8	Security Training Standards	NIA

3.3 **Statutory Responsibilities**

Notwithstanding the above responsibilities, in line with the requirements of the MISS document (Minimum Information Security Standards), the Municipal Manager remains responsible in as far as all security matters are concerned, He/she may, however, delegate all or certain security responsibilities to the Heads of Departments.

3.4 **Administrative Responsibilities**

3.4.1 It is not practically possible for the Municipal Manager to personally address the security needs of each Department. Therefore the authority and responsibilities in respect of security administration are delegated to the Managers in the Departments. These officials are responsible for administering all aspects of security within their departments. The Managers bear the overall co-ordinating function on behalf of the Municipal Manager.

Functional Responsibilities

3.5.1 The functional performance of various security measures and procedures is primarily the responsibility of each and every employee of the Endumeni Municipality, irrespective of rank. All managers and supervisors must ensure that all personnel, assets and information under their control are safe and security at all times and that the relevant procedures are adhered to.

3.5.2 The Roles and Functions of the Managers

3.5.2.1 The authority to, co-ordinate and take the necessary actions in all security related matters in the Municipality is delegated to the Managers who shall be responsible for the following:

- (a) Manage the total security function (personnel, document, physical communication, computer and surveillance security) in the Municipality
 - Together with the Manager's forum, draft the Municipal Security Policy and effect changes thereto
 - Brief the Management Executive Committee (Mexco) from time to time on all security related matters
 - Advise the Management Executive Committee about amendments to the Municipal Security Policy
 - Advise Management Executive Committee about the security implications of its decisions
 - Ensure that corrective/disciplinary steps in cases of non-adherence are initiated, in line with the policy of misconduct
 - Liaise with NIA for advise, assistance and information regarding information security
 - Report to NIA all incidents or suspected incidents of security breaches and/or leakages of sensitive information, for investigation. He/she will also be responsible for keeping record of all security incidents (e.g. leakages, thefts, burglaries, tampering with security systems, hacking, etc) in the municipality
 - Ensure that all departments run security awareness programmes
 - Monitor the extent of adherence/compliance to the security policy and measures in the Municipality, (including that officials with access to sensitive information are vetted)
 - Ensure that physical security appraisals are conducted in departments as well as proper implementation of recommendations, in consultation with the relevant authorities;

- Ensure the effective implementation of all security measures in the Municipality (e.g. security communication and communication channels and vetting of staff, access control, etc.)
 - Ensure the proper administration of vetting applications in the Municipality
- (b) The Departmental Managers are further responsible for the facilitation and advising Municipal Departments on all security related matters and is the link between the Municipality and the National Intelligence Agency and other relevant national security structures.
- (c) Furthermore, he or she must ensure that security policies, procedures and standards are maintained throughout the Endumeni Municipality and must promote timely dissemination of instructions and the reporting of incidents to the Municipal Manager.

3.5.3 The Roles and Functions of the Departmental Security Components

3.5.3.1 Each Department should establish its own Internal Security Administration Component, which will be headed by a Manager, to perform the implementation of personnel, information and physical security measures, as well as security training.

3.5.4 The Duties of Security Officers

3.5.4.1 The performance of the physical security duties of access control and guarding services are performed by members of the in-house Security Officers or by members of private companies in contract with the Endumeni Municipality.

3.5.5 The Duties and Functions of Departmental Security Administration Components

The Security Administration Components in the Departments are responsible for the practical and theoretical application and implementation of physical measures for the security of personnel, information and property and include but are not limited for:

- (a) Access Control
- (b) Searching of vehicle as well as hand baggage
- (c) Patrolling of buildings, premises and perimeters
- (d) Monitoring of emergency- and alarm systems
- (e) Escort services for protection purposes
- (f) Security evaluations

- (g) Needs assessments
- (h) Advice on physical security measures
- (i) Awareness programs
- (j) Policy adjustments to suit the specific departments
- (k) Monitoring and reporting
- (l) Research
- (m) Liaison with role players in the security environment
- (n) Facilitating on emergency and evacuation planning procedure
- (o) Training of security personnel

3.5.6 The Roles of Managers in the Municipal Departments

3.5.6.1 3.8 The managers in the departments are responsible for the following:

- (a) Manage the total security function in their own departments (personnel, document, physical, communications, computer and surveillance security);
- (b) Brief the Municipal Manager from time to time on all security related matters;
- (c) Advise Municipal Manager about the security implications management decisions;
- (d) Identify all risks and threats to the security of the department and advise the Municipal Manager of these;
- (e) Devise security measures and procedures for the department based on the Municipal Security Policy;
- (f) Evaluate and improve security measures and procedures in department.
 - Create, develop and maintain a security training capacity for the department and conduct security sessions of all officials;
 - Run a security awareness programme in the department;
 - Monitor the extent of adherence/compliance to the Municipal Security Policy and measures within the department;
 - Initiate corrective/disciplinary steps in cases of non-adherence with the policy about misconduct;

- Conduct physical security appraisals in the department and ensure proper implementation of recommendations, in consultation with relevant authorities;
- Liaise with the relevant authority about all physical security needs, problems, etc., to ensure effective security (e.g. key control, access control, and/or security equipment/installations);
- Ensure the effective implementation of all security measures within the department (e.g. security and communication channels and vetting of staff, access control, etc);
- Crypto management and appointment of all necessary officials for crypto administration.

3.7

The Roles and Functions of the Municipal Security Managers' Forum

3.7.1 In addition to the above, a Municipal Security Managers Forum shall be formed which will consist of managers from municipal departments. The Security Managers' Forum shall be headed by a Manager in the Municipality. The functions of the Committee shall include:

- Drafting the Municipal Security Policy and effect amendments as and when necessary;
- Brief the Management Executive Committee from time to time;
- Co-ordinate security training capacity in the departments;
- Co-ordinate Security Awareness programs in the departments;
- Monitor the extent of adherence/compliance to the Municipal Security Policy in the Departments;
- Evaluate the effectiveness of the Security Policy

CHAPTER 4

DOCUMENT SECURITY

These prescriptions apply to documents which contain sensitive information and by its nature need to be classified Confidential, Secret and Top Secret

Classification and Reclassification of Documents

- 4.1.1 Departments have at their disposal intelligence/information that is to some extent sensitive in nature and obviously requires security measures. The degree of sensitivity determines the level of protection, which implies that information must be graded or classified accordingly. Every classification necessitates certain security measures with respect to the protection of sensitive information which will be known as classified information.
- 4.1.2 The responsibility for the grading and regarding of document classifications rests with the department where the documents have their origin. This function rests with the author or head of the department or his delegate(s).
- 4.1.3 The classifications assigned to documents shall be strictly observed and may not be changed without the consent of the head of the department or his delegate.
- 4.1.4 Where applicable, the author of a classified document shall indicate thereon whether it may be reclassified after a certain period or upon the occurrence of a particular event. This option is to be applied consistently upon the award of a classification.
- 4.1.4.1 Should the author of a document on which there is no embargo, reclassify such document, he must inform all addressees of the new classification
- 4.2.4.2 The receiver of a classified document who is of the opinion that the document concerned must be reclassified, must obtain oral or written authorization from the author, the head of the department or his delegate(s). Such authorization must be indicated on the relevant document when it is reclassified;
- 4.1.5 The classification of a document or file will be determined by the highest graded information it contains. The same classification as that of this original must be assigned to extracts from classified documents, unless the author consents to a lower classification.
- 4.1.6 Every document must be classified on its own merit (in accordance with its own contents) and in accordance with the origin of its contents, and not in accordance with its connection with or reference to some other classified document, provided that where the mere existence of a document referred to is in itself information that calls for a higher security classification than the document containing the reference, the latter document must be classified accordingly.

4.1.7 The author of a document must guard against the under classification, own classification or unnecessary classification of documents. The head of an institution or his/her delegate must on a regular basis test classifications of documents generated in his/her institution against the criteria applicable to the relevant classification.

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

4.1.8.1 Documents and Bound Volumes

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

4.1.8.2 Copies, tracings, photographs, drawings, sketches, etc.

4.1.8.2.1 Security classifications shall be indicated on such documents by means of rubber stamps or other suitable means. The exact position of the mark may vary, depending on the nature of the document, so that essential details shall not be obscured by the stamp. An effort must, however, be made to make the document as clearly as possible, so that the mark will immediately attract attention.

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

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

4.1.8.4 Tape recordings and documents on which no marks can be made. 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. The nature and classification of the contents clearly marked on the outside of the container.

4.1.8.5 Files. A clear distinguishing mark, the significance of which is known to those who deal with the file concerned, should be placed on both the front and the back cover of Secret or Top Secret files.

4.2 **Criteria for Classifying Documents**

4.2.1 The following criteria must be used when classifying documents:

Confidential: This is limited to information that may be used by malicious/opposing/hostile elements to harm the objectives and functions of an individual and department or any sphere of government;

Secret: When the compromise of information can result in the disruption of the planning and fulfilling of tasks, i.e. the objectives of a state or department in such a way that it cannot properly fulfil its normal functions; and can disrupt the operation co-operation between departments in such a way that it threatens the functioning of one or more of these departments;

Top Secret: This is used when the compromise of information can result in:

- The functions of a state, provincial and/or local government department being brought to a halt by disciplinary measures, sanctions, or mass action;
- The severing of relations between state;
- A declaration of war.

4.3 **Uncertainty about the Status of Documents**

Where there is uncertainty regarding the level of classification to be accorded a particular document the author(s) must refer the matter to the head of the department who shall make an appropriate determination.

4.4 **Access to Classified Information**

4.4.1 The following persons have access to classified information:

- (a) A person who has an appropriate security clearance or who is by way of exception authorized thereto by the head of the department or his/her delegate, with due regard being paid to the need-to-know principle;

- (b) Persons who must necessarily have access to that classified information in the execution of their duties (the need-to-know principles) – on condition that a suitable clearance has been issued or authorisation has been granted;
- (c) Persons such as stand-in typists/secretaries and personnel at smaller centres who in general do not have access to classified material and who do not have a relevant security clearance, but are expected to have access to this information on an ad-hoc basis owing to the circumstances, on condition that the prescribed oath/declaration of secrecy was taken;

4.5 The state's restriction of classified information is done in accordance with among others, the Protection of Information Act, Administrative Justice Act, Section 36 of the Constitution and other related Acts.

4.6 **Municipal Executive Council Documents**

All MEC documents, including correspondence relating to MEC matters, memoranda and annexures thereto, agendas, recommendations/resolutions must be classified as secret documents in the following manner:

S top and bottom pages of the first cover;

S Top and bottom pages of every following page including annexures

4.7 **Private/Personal and Confidential**

The mark "Confidential" in respect of staff matters must not be confused with the "confidential" used for security reasons. When the work "confidential" is used to refer to a personal matter, it must always be accompanied by the word "private" so that it reads "private and confidential".

4.8 **Allocation of Higher Classification (Upgrading)**

4.8.1 Nobody may upgrade a classification without the precedent consent of the drafter. If an upgrading does occur after consent, the drafter must also upgrade the copies. If upgrading is done without the consent of the drafter, then the drafter must be informed in writing and requested to upgrade the copies.

4.8.2 If upgrading is done by a non-departmental institution, the drafter must ascertain the circumstances under which it was done. Furthermore the same rule applies in respect of the copies, as explained previously.

4.9

Dealing with Classified Matters from Foreign Countries

Security instructions received from any institution of a foreign country, which concerns the treatment of classified issues of such country, must be obeyed except where such instructions are in conflict with those of our instructions and policies.

4.10

Handling of Classified Documents

4.10.1 All classified documents must be stored in accordance with instructions while not in use. All departments must appoint a person who shall be responsible for registering all classified documents.

4.10.2 All incoming classified documents, including official, classified post marked "Personal" must be received and noted in a register by persons with the appropriate clearance. The object of such registration is to enable total control over such documents.

4.10.2.1 Officials who usually receive the incoming post of an institution (e.g. registry officers) must hand the unopened inner envelope of incoming classified correspondence to the appropriate official(s) who is/are authorized to open correspondence in a certain category. The latter is/are responsible for entering the correspondence concerned in the prescribed register.

4.10.3 All classified documents that are dispatched, made available or distributed, must be subjected to record keeping in order to ensure control thereof.

4.10.3.1 Measures must be taken to ensure that classified documents are not physically taken from one institution to another and/or informally handed to a member of another institution during a contact visit, in this way evading prescriptions for the registration of incoming and outgoing post.

4.10.3.2 All departments must draw up standard registers in which the particulars of classified postal material are to be entered. Over and above this, the Municipal Manager's office and offices of Heads of Departments and all offices dealing mostly with classified documents must also draw up such registers. These registries must be inspected by Managers on monthly basis. Registers for the particulars of postal material classified as Secret and Top Secret are to be classified accordingly. The registers must include the following particulars:

4.10.3.2.1 **Particulars of incoming post:** Serial number of the entry; Date of receipt; From whom received; Registered postal material and reference number; Classification (C/S/TS); Subject/heading' Disposal: File number, Recipient (signature); Further dispatch (serial number of the entry for outgoing mail in the register); Destruction (date and signature);

4.10.3.2.2 **Particulars of outgoing post:** Serial number of the entry; Date of dispatch; Reference number and date of the document; Classification; Subject/heading; Dispatched/addressed to; Nature of dispatch (courier, by hand, registered post, facsimile, by computer); Registered number of postal material; Signature of the recipient (courier, registration, person dispatching); Receipt number; Date when receipt was obtained. These registers must be inspected on a monthly basis by Managers in the departments.

4.10.4 When Secret and Top Secret documents are distributed, dispatched or made available, they must be accompanied by a receipt voucher signed by the addressee, the receipt of which must again be controlled by the sender. The receipt voucher is classified only if the subject/heading of the document itself is classified, in which case the classification must agree with that of the document.

4.10.5 All Secret and Top Secret documents must be given copy numbers and an indication must be given of the number of copies produced, e.g. Copy 1 of 7 copies. The copy number should appear on the first page of each document, in the upper right-hand corner.

4.10.6 In the case of Council documents sent via the Managers, it is the responsibility of officers responsible for Council matters to allocate copies to documents retrieved from the Managers as per the distribution list issued by the Council.

4.10.7 A serial number must be allocated to every document filed in a classified file as is indexed on a page attached to the inside of the file cover, together with the name/heading of the document concerned.

4.11 **Transmitting Documents by Means of Facsimile**

4.11.1 When classified documents are transmitted by means of facsimile, on facsimile machines equipped with encryption must be used;

4.11.2 Classified reports may only be handled by a suitably cleared operator;

- 4.11.3 The Cryptographic equipment and facsimile machines must be kept in a room that is manned at all times while it is unlocked or in use by a suitably cleared, trained and appointed official, while care has to be taken that reports received through this apparatus are not accessible to unauthorized persons;
- 4.11.4 A record must be kept of the transmission and receipt of classified documents;
- 4.11.5 After receiving a message, receipt must be acknowledged immediately. The recipient shall ensure receipt of all pages;
- 4.11.6 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, he/she shall immediately transmit an acknowledgement of receipt to the sender;
- 4.11.7 The recipient shall, on his/her copy, note the copy number as indicated on the distribution list;
- 4.11.8 Effective control must be exercised over "open" facsimile machines to ensure that these are not used for the transmission of classified documents.

4.12 **Transmitting Documents by Computer**

- 4.12.1 Encryption shall be applied with respect to the computerised transmission of classified documents.
- 4.12.2 A record shall be kept of the classified document transmitted and received, provided that the recipient of documents must always acknowledge receipt of classified documents. It must also be remembered that all magnetic media must be regarded as documents and handled as such.
- 4.12.3 Such documents must be supplied with copy numbers.

4.13 **Dispatching Classified Documents by Courier**

- 4.13.1 The registry departments where classified documents are received and dispatched must have a mail-list wherein incoming classified documents could be acknowledged. The mail-list must have an official stamp.
- 4.13.2 All classified documents must be noted in a register indicating the title-description of the document and the date and time of dispatch, and must be handed over against the signature of the courier. In this regard, the courier refers to in-house drivers/messengers and outside courier agencies.
- 4.13.3 A courier must convey classified documents in a safe locked container, which must have a combination lock.

4.13.3.1 Secret and top secret documents (and where necessary also sensitive confidential documents) should be delivered locally only by hand (i.e. by a courier). The following shall be adhered to:

- Couriers must have at least a Confidential security clearance
- Where possible the courier must be accompanied by a second person
- All classified material must be conveyed under safe conditions, in an attaché case with a code or combination lock (particularly if the courier is not accompanied by a second person)
- The courier must obtain an appropriate receipt for the material
- On the return of the courier the receipts for classified deliveries must be checked by a responsible officer.

4.13.3.2 Control must be exercised over the time taken by the courier to deliver the documents. Upon receipt, the recipient of such documents must check that the documents have not been compromised.

4.13.3.3 Couriers must be able to identify themselves when fetching or dispatching post.

4.14 **Dispatching Classified Documents by Mail**

4.14.1 Classified documents in the Secret and Top Secret categories that cannot be dispatched by courier may, as an exception, be mailed on provision that it be sent by registered mail and then only with the express permission of the head of the institution or his delegate.

4.15 **Sealing of Classified Documents Before Dispatch**

4.15.1 Classified documents that are dispatched (excluding by facsimile and computer) must be sealed and handled in the following way:

4.15.1.1 A receipt to be signed by the addressee and returned to the sender, must be attached to the document and placed in the inside envelope. This does not apply to “Restricted” documents.

4.15.1.2 Classified documents must always be dispatched in a double envelope/cover, i.e. in an envelope placed within another (excluding “Restricted” documents). The following process shall be followed:

- The seams of the inside envelope must be properly sealed with paper seals, counter signed 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).
- 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 document must appear clearly on the front of the inside envelope.
- The security classification of the document must be indicated clearly on the front and the back of the envelope by means of a rubber stamp.

4.15.1.3 The outer envelope should bear only the name and address of the addressee and the name and address of the sender. Under no circumstances should there be an indication of the nature or classification of the contents, since this could attract undesirable attention to the document.

4.15.1.4 Persons who normally receive incoming post in an office (such as the registry officers) must make sure that they know who is authorised to open incoming classified correspondence in each particular category and must hand the inner envelope unopened to the authorized officer(s) concerned.

4.16 **Bulk Conveyance of Classified Documents**

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

4.16.2 **Diplomatic Bags**

4.16.2.1 Classified and unclassified documents to be dispatched to RSA mission abroad or departmental representatives there must be sent to the Department of Foreign Affairs for dispatch, whether in diplomatic or airfreight bags. In order to ensure that this provision is complied with, the Department of Foreign Affairs may therefore, where it is considered, necessary, examine the contents to ensure that the mentioned provisions are complied with.

Storage of Classified Documents

- 4.17.1 Classified documents that are not in immediate use must be locked away in a manner prescribed in the following paragraphs below. In this regard all offices dealing with classified documents must be fitted with appropriate safe storage facilities:
- 4.17.1.2 A shortage of facilities for safekeeping of documents does not exempt anybody from the responsibility of safeguarding documents to the maximum. Classified documents may not be left displayed in offices for unauthorized perusal.
- 4.17.1.3 No indication of the subject or level of security of the contents of any strongroom, safe, steel cabinet or container, used for the safeguarding of classified documents, may be displayed on the outside of it.
- 4.17.1.4 When visitors, messengers, etc., enter an office or workplace, the occupant of the office must lock away such documents or cover them so that nobody can read the contents or even the file headings.
- 4.17.1.5 No cleaning or repair may be done to, or in an office in which classified documents are kept or normally handled, without the occupants being present. A person with a security clearance to the appropriate level must be appointed to supervise in respect of the above, when the occupant of an office is absent;
- 4.17.2 The doors of all offices in which classified documents are kept must at least be fitted with security locks.
- 4.17.3 There must be proper control over access to and effective control over movement within any building or part of a building in which classified information is handled. The identification of visitors, the issue of visitors' cards or temporary permits, the escorting of visitors, the provision of identity cards for officers/employees working in the building/offices and the use of related documents and registers for this purpose are prerequisites for effective control over access to and within a building or part of a building.
- 4.17.4 Effective control must be instituted over access to security areas in a building such as cryptographic and computer centres, the registry (where secret and top secret documents and files are kept) and other areas identified as sensitive. An access register must be instituted and kept up to date for all persons/officers not normally working in these areas.

- 4.17.5 Where necessary (depending on the sensitivity of the classified material kept or dealt with in a particular room or division) doors, windows, fanlights, passages, stairs, etc., giving access to the room or division should be equipped with locks, bolts, iron bars or metal blinds of adequate strength, as the case may be. In some cases it may be sufficient to equip one room in a building in this way to serve as registry or storeroom for classified material.
- 4.17.6 Apart from taking the precautions mentioned above, all the doors of any room in which classified secret or top secret material is dealt with or handled must be fitted with security locks and must be locked when it is vacated, even for a short period, by the person(s) using the room.
- 4.17.7 In the officer(s) leave the room for a longer period, e.g. during the lunch hour, all classified secret and top secret material must be locked away in a safe or metal cabinet which is of adequate strength and equipped with a security lock.
- 4.17.8 Officers dealing with classified documents must before they leave for home satisfy themselves that all such documents have been locked in a safe place.
- 4.17.9 When classified documents are not in use, it must be stored in the following way:
- Confidential: Reinforced filing cabinet
 - Secret: Strongroom or reinforced filing cabinet
 - Top Secret: Strongroom, safe or walk-in safe
- (Steel cabinet is reinforced if it has iron bars and can be locked with a pad lock)
- 4.17.10 The key to any building, part of a building, room, strongroom, safe, cabinet or any other place where classified material is kept must be looked after with the utmost care and effective key control must be instituted.
- 4.17.11 The keys to safes and strongrooms must be kept in safe custody and must be manned by the unit Director or his/her delegate.
- 4.17.12 If a strongroom or safe is fitted with a combination lock, the combination must apart from being reset when it is purchased, be changed at least once every three months, or on the following occasions:
- When it is suspected that it has been compromised;
 - On resumption of duty after a continuous period of absence, whether on vacation leave or for official reasons, if the combination had necessarily to be made known to some other person for use during the period concerned;
 - When a new user takes over.

4.17.13.1 Combinations may be compromised by:

- Unauthorised persons noting the combination through observation when the lock is opened;
- Failure to set the combination in accordance with the manufacturer's specifications;
- Failure to change the combination after a reasonable period

4.17.13.2 Precautions must therefore be taken by the authorized user to ensure that no other unauthorised person is present when the new combination is set or the lock is opened. When a combination is reset, the following rules should be adhered to:

- The figures making up a specific combination should not be used more than once in succession, even if they are in a different order. Avoid the use of numbers with some personal significance, e.g. age, date of birth, telephone numbers, street addresses and numbers of safes, etc. Also avoid the figures zero (0), five (5), ten (10) and multiples of the last two. High and low numbers should preferably be used alternately (e.g. 68-13-57-11).
- Only the user may set a combination lock

4.17.13.3 Knowledge of a combination should be restricted to the minimum number of persons desirable on the grounds of operational requirement, e.g. in the case of a communal safe.

4.17.13.4 After the combination has been reset, the new combination must be handed to the Head of Security or other person designated for the purpose in a sealed envelope for safe custody, so that he can complete the combination lock register.

4.17.14 Access to any controlled building, part of a building or room which classified information is handled/stored outside normal office hours should be prohibited to all persons who do not work there. Repairs to and the cleaning of such premises must take place in the presence and under supervision of the persons who work there. Persons who have to gain access to a building after hours must be duly authorized accordingly by the Head of the Institution or his delegate. The Head of Department must take appropriate steps to arrange access and record keeping.

4.18 **Registries and Files**

4.18.1 Central Registries for Receiving of Incoming Mail and Dispatching of Outgoing Mail

4.18.1.1 All departments should have one central/main registry 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 (whether electronic or hard copy).

- 4.18.1.2 In view of the logistical arrangements in our Municipality and the fact that most departments occupy more than one building, all buildings occupies must have a central/main registry unity which will service that department or a particular unit of the department located away from the head office.
- 4.18.1.3 Over and above the central/main registry offices, the Department which deal mostly with classified documents should have their own registry units which should be manned by officials with relevant security clearance.
- 4.18.1.4 Internal distribution should be reflected in registers for incoming and outgoing mail, that should be kept at all other registries or offices where internal mail are received. These registers should contain the following particulars:

Particulars of Incoming Post: Serial number of the entry; Date of Receipt; From whom received; Registered postal material and reference number; Classification (C/S/TS); Subject/heading; Disposal; File number; Recipient (signature); Further dispatch (serial number of the entry for outgoing mail in the register); Destruction (date and signature).

Particulars of outgoing post: Serial number of the entry; Date of dispatch; Reference number and date of the document; Classification; Subject/heading; Dispatched/addressed to; Nature of dispatch (courier, by hand, registered post, facsimile, by computer); Registered number of postal material; Signature of the recipient (courier, registration, person dispatching); Receipt number; Date when receipt was obtained.

- 4.18.1.5 Apart from being registered, a system of route cards or similar, should be implemented to ensure that a document can be traced at any time.
- 4.18.1.6 Outgoing mail should be forwarded to the central registry from where it will be dispatched. This forwarding and dispatching must be subject to the control measures as described in the MISS elsewhere.

4.18.2 **Access to Registries**

Access to registries should be controlled. No unauthorized person (any person that has no direct line functional responsibility inside the register) must be allowed inside.

4.18.3 **Management of Files**

- 4.18.3.1 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.

- 4.18.3.2 The particulars appearing on the file should be at least: the name/topic of the file, the file number, the classification, and who are/is authorized to have access to that file.
- 4.18.3.3 A register should be kept of all files opened/inexistence. 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 file number.
- 4.18.3.4 a file must be classified according to the highest level of classification of the documents it contains.
- 4.18.3.5 The classification mark must be affixed on the file as described elsewhere in this document.
- 4.18.3.6 Classified files must be stored in facilities as prescribed for classified documents.
- 4.18.3.7 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 document.
- 4.18.3.8 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 taken out of the registry (which should not be common practice), an indication must be made on the sub-file to whom the main file has been issued, and when, 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.
- 4.18.3.9 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 are on standard (as prescribed) and that the return of the file is followed up on a daily basis by the head of the registry.
- 4.18.3.10 Only authorized persons may be allowed access to classified files. Internal policy should dictate who may authorize such access, subject to the need-to-know principle.

4.19 **Removal of Classified Documents from Premises**

- 4.19.1 Classified material (with the exception of “Restricted” documents) may not be taken home without the written approval of the Manager of the Department and a list of the documents to be removed must be handed to the person in control of record keeping. Persons may take classified documents home only if they have proper lock-up facilities, in other words, if a person has no such facilities, the documents may not be kept at such a person’s home for the purpose of work after hours.

- 4.19.2 Classified documents taken out of a building with a view to utilization at meetings or appointments must be removed in a lockable security attaché case. In this regard all departments, offices, sections dealing with classified documents must acquire such lockable security attaché.

4.20 **The Typing of Classified Documents**

- 4.20.1 Classified documents may be typed only by persons having the appropriate security clearance. The documents may not be sent in office files nor hand delivered. Such typing must be done in a manner that will ensure that the information is not divulged to unauthorised persons.
- 4.20.2 Drafts of classified documents, typewriter ribbons, cassettes and copies and floppy disks must at all times be treated as classified documents.

4.21 **Destruction of Classified Documents**

- 4.21.1 In line with the provisions of the National Archives Act, original copies of classified documents, shall only be destroyed with the prior authority from the Director of State Archives.
- 4.21.2 Only photostat copies of such a document may be destroyed without such authority. However, if the author(s) or signatory to the documents has written something on the document, such a document becomes a new original.
- 4.21.3 Where destruction has been properly authorised, 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 officer who has destroyed the documents must give a certificate of destruction of the documents concerned to the head of the institution or his delegate. The state archives department must be involved or informed when a document is destroyed.
- 4.21.4 The process of destruction must be such that reconstitution of the documents destroyed is impossible.

4.23 **Making Photocopies of Classified Documents**

- 4.23.1 All mechanical/electronic reproduction appliances should be properly controlled to prevent the unauthorised or uncontrolled copying of classified documents. This apparatus must therefore either be centralised or distributed and be under the direct control of an authorised and aptly cleared officer;
- 4.23.2 The relevant department must keep a record of all the reproductions of classified documents at its disposal. The register must contain the following particulars: Date, Person requesting copies/reproduction, Classification, File reference, Heading/nature of documents, Purpose of the copies, Number of copies, meter reading before and after copying.
- 4.23.3 Oral or written authorization for the copying of secret and/or top secret documents by the author, head of the institution or his delegate(s) is required for the copying of secret and/or top secret documents. Such authorization must be indicated on the original document.

- 4.23.4 Copies of all secret and top secret documents must receive 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 addenda must be numbered in accordance with the relevant classified document. All addressees/department, individuals concerned and the corresponding copy numbers must be written in the file and record copy. Alternatively a distribution list can be attached to all copies of the relevant document concerned, indicating the addressees and the applicable copy number.

CHAPTER 5

PERSONNEL SECURITY

GUIDELINES WITH RESPECT TO SECURITY VETTING

5.1 General

- 5.1.1 In conducting its day to day business, the Municipality often deals with sensitive information which must be protected.
- 5.1.2 Towards the above end, this must be taken into consideration right from the beginning during the recruitment process so that people employed to handle such information have the necessary calibre and integrity. In this regard, when a post is advertised the incumbent of which will be expected to deal with classified information/documents, it should be indicated in the advertisement that the successful applicant or candidates considered suitable for appointment will be required to undergo a security clearance process.
- 5.1.3 Before any appointment is made, whether or not the incumbent will be dealing with classified information and irrespective of the rank, reasonable measures must be taken by the personnel section of a department to verify the credentials of the prospective incumbent and the authenticity of certificates obtained. It is the responsibility of the personnel sections to verify such information and when they submit recommendations for appointments, indicate that they have satisfied themselves regarding the above.
- 5.1.4 For officials who will be dealing with classified information, a clearance letter has to be issued by NIA before a suitable candidate is appointed.
- 5.1.5 Officers who refuse to undergo a security screening or those in respect of whom a positive clearance has not been issued, can normally not be utilized in such a post and their utilization will be reconsidered. For people serving a probation period who have to deal with classified information/documents, the result of the security vetting will have to be considered before the probation is confirmed. In case the probation period ends before the result of the security test are released, the officer must be notified in writing that the appointment is only temporary, pending the result of the investigation (screening).
- 5.1.6 The level of clearance will be determined by the nature of the information that an officer deals with. In this regard, the following rules apply:

S: All officials dealing with Council documents have to be issued with a secret clearance certificate. This includes executive secretaries and general assistant.

S: All officials in the registry departments, as well as messengers and personnel dealing with confidential documents must be issued with at least a confidential clearance.

5.1.7 All departmental managers must be issued with a Top Secret clearance.

5.1.8 In this regard, departments must bear all the financial costs incurred during vetting of in-house personnel e.g. finger print taking fees while people who are considered for employment must pay finger print fees out of their pockets.

5.1.9 The degree of security clearance given to all other staff is determined by the content of and/or access to classified information entailed by the post already occupied/to be occupied by the person.

5.1.10 A declaration of secrecy should be made on an official form, attached as annexure "A", by an applicant to any municipal post, before he/she is appointed or during the appointing process. Irrespective of whether or not he will be dealing with classified information.

5.1.11 Managers of Departments will not be vetted, unless the Municipal Manager so requests or the relevant contract so provides. All staff members and any other individuals who should have access to classified information, must be subjected to security vetting.

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

5.2 VETTING CRITERIA

5.2.1 The vetting/screening will be as determined by NIA, however 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 person's vulnerability to blackmail or bribery or subversion and his loyalty to the Municipality do. This also includes compromising and behaviour.

5.3 Security Screening in respect of Immigrants and Persons with More than One Citizenship

5.3.1 The following levels of security clearance in respect of the vetting of immigrants and persons with more than one citizenship were taken from the MISS document.

5.3.2 **Confidential Clearance.** A confidential clearance may be considered in respect of an immigrant who has been resident in the RSA for ten consecutive years of which at least those five years preceding the clearance were spent as a South African citizen. He/she must provide sufficient proof that any former citizenship has been relinquished.

5.3.3 **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/her former citizenship.

5.3.4 **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 the condition that such a person has relinquished his/her 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.

5.3.5 **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.

5.3.6 **Persons without Valid Identification Documents:** No clearance can be issued in the following cases:

5.3.6.1 Any person who is not in possession of a valid identification document or residence permit for the RSA;

5.3.6.2 Naturalised RSA citizens who have not applied for a new identification document after naturalization, since the document that was issued before naturalization expires on naturalization.

5.3.7 **Employing Immigrants Who Do Not Meet Clearance Requirements**

5.3.7.1 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 utilized 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 employing department may authorize that the immigrant be used in the post on the condition that the employing department must:

- Submit a certificate to the National Intelligence 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;

- 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;
- Declare that it accepts full responsibility for compliance with the security requirements connected with the employment of such immigrant;
- Ensure that no classified information or material that is not needed for the performance of his duties comes into the position of the incumbent of the post; and
- Reconsider the authorization every year and relate in writing to both the National Intelligence Agency and the responsible screening authority any incident which could pose a threat to security or any incidence which may bring his/her security competence into question.

5.3.7.2 **Take Note:** When the person concerned changes his/her posting, the authorization is automatically terminated.

5.3.8 In respect of immigrants already employed in sensitive positions and in whose case the conditions laid out in Chapter 5, paragraph 5.3.6 above have not yet been complied with, the employing department must immediately give effect to those conditions as set out in paragraph 5.3.6

5.4 **Screening/Vetting of Persons Who Have Lived/Worked Abroad for Long Periods**

5.4.1 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 to a government or semi-government institution or a national key point for employment, such a person is temporarily not eligible for any grade of security clearance. Applications for 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:

5.4.1.1 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.

5.4.1.2 A Secret clearance after three years back in the RSA;

5.4.1.3 A Top Secret clearance after two years back in the RSA.

5.5

Security Screenings: Contractors Supplying Services to Departments

5.5.1 Departments should indicate expressly in documents sent to the State Tender Board or private contractors whether there are security implications that should be taken into account in advance when they perform their duties for the department/institution involved. If there are such implications, reasons 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. Obtaining 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:

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.”

5.5.2 The security responsibilities of the contractor will be determined by the department/institution concerned.

5.6

Procedure for Requesting Security Screenings

5.6.1 Requests for security screening and re-screening must be submitted to the appropriate screening authority through the Departmental Security Managers on the prescribed form accompanied by a set of clear fingerprints.

5.6.2 The requesting department should provide the screening authority with a post description of the employee concerned and an indication of the access he/she has/will have and with all other facts that may influence the issue of a clearance.

5.7

Period of Validity of Security Clearances

5.7.1 The head of the 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 rescreened every five (5) years and every ten years in respect of a Confidential clearance.

5.7.1.1 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 certificate;

5.7.1.2 This arrangement does not preclude rescreening 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.

5.8. Transferability of Clearances

- 5.8.1 When an officer changes his employer, the responsibility for deciding whether an applicant's existing clearance will be accepted or whether the rescreening of such an officer will be requested in the prescribed way rests with the new employer.
- 5.8.2 However, for the purpose of meetings and other co-operative functions clearances are transferable. The employing institution is responsible for informing the chairperson of such a meeting in writing as to the level and period of validity of the clearances of the representatives involved.

5.9. Responsibilities of the Screening Authority

- 5.9.1 The screening authority will investigate and advise on the security competence of a person on the basis of prescribed guidelines.
- 5.9.2 After the investigation the screening authority will merely make a recommendation regarding the security competence of the person concerned to the head of the requesting institution, and this should in no way be seen as a final testimonial as far as the utilization of the person is concerned.

5.10. Responsibilities of the Head of the Requesting Institution

- 5.10.1 The head of the department or his delegate 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.
- 5.10.2 Notwithstanding a negative recommendation from the screening authority, for whatever reason, the head of the department may still, after careful consideration and with full responsibility, use the persons concerned in a post where he/she has access to classified matters if he/she is of the opinion that the use of the person is essential in the interest of the RSA or his/her institution, on the understanding that a person satisfying the clearance requirements is not available.
- 5.10.3 When any person is utilized without a clearance, the responsible screening institution and the National Intelligence 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 screening authority concerned.
- 5.10.4 Heads of institutions whose officers 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.
- 5.10.5 Further, it is also the responsibility of the head of the department or his/her delegate to:
- Ensure that there is continuous supervision of persons in respect of whom security clearances have been issued;

- Present security awareness programmes for his/her employees and to warn staff members not to supply personal particulars of colleagues/officers to unauthorised persons;
- Ensure that persons dealing with classified matters sign the prescribed declaration of secrecy;
- Pertinently bring to the attention of the officers working with classified matters any other legislation, regulation and/or orders that entail secrecy and/or the protection of activities, installations, etc., of any particular institution;
- 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;
- To ensure that all classified documents in the possession of the person concerned are returned when such person resigns or leaves the service; and
- To ensure that no information comes into the possession of an individual that is not essential for the performance of his or her duties.

5.11 **Officers Travelling Abroad**

- 5.11.1 In the event where an official with a clearance travels abroad, the head of the institution employing the official or his/her delegate must keep a thorough record of such visits.
- 5.11.2 When officials are travelling abroad they must be on their guard against any attempt by a foreign intelligence service to recruit them. If a person is approached, he or she must, immediately on returning, report the fact to the head of the institution or his/her delegate for transmission to the responsible screening authority and the National Intelligence Agency. While travelling, officials should maintain a low profile and be careful not to place themselves in compromising situations.

5.12 **Security Awareness**

- 5.12.1 The Municipal Security Managers' Forum must on a yearly basis develop and monitor security awareness program.
- 5.12.2 Managers in departments are responsible for implementing the security awareness program in a manner that suits their conditions;
- 5.12.3 Frequent effort must be made to draw attention of personnel to the importance of security and the strict execution of the security programme.

CHAPTER 6

COMMUNICATION SECURITY

- 6.1 Communication may be divided into two main categories:
- 6.1.1 Communication taking place with the aid of communications equipment, telex equipment, computer equipment, radio and facsimile equipment and the telephone. Departments must develop their own communication security policy which shall serve as the minimum communication standard;
 - 6.1.2 Communication taking place without communications equipment, i.e. mainly personal communication.
- 6.2 Classified information should be transmitted only under the following conditions:
- 6.2.1 Via acceptable and approved apparatus as stipulated in Chapter 4 section 4.11 of this document.
 - 6.2.2 The necessary encryption as prescribed, must be present.
- 6.3 Personal communication of a sensitive or classified nature must necessarily be subject to strict self discipline on the part of the communicator. In this regard the following guidelines apply:
- 6.3.1 The need-to-know principle;
 - 6.3.2 Such conversation should take place in such a way that sensitive information/intelligence does not come into the possession of unauthorized persons or persons who happen to overhear;
 - 6.3.3 Places such as offices, conference rooms, etc., where sensitive or classified matters are discussed on a regular basis should be subject to:
 - Proper and effective access control (e.g. outside maintenance personnel and cleaners);
 - Regular electronic surveillance counter measures (sweeping). (In this regard the National Intelligence Agency can be contacted in the case of government departments, parastatals and private institutions. The SASS, SANDF and the SAPS are responsible for electronic surveillance counter measures with regard to their own environment).
- 6.4 The Chief Directorate Security of NIA or SACSA may be approached through the Municipal Manager in the Municipality for further advice and guidance in respect of communication security needs.
- 6.5 **Communication to the Media**
- The Municipality has a duty to protect information. The information that the officer employed get hold of in the course of their duty is the property of the Municipality and can only be released through proper channels. The designated officers in the communication departments as well as the spokespersons of the Council are the only people that have the authority to communicate with the media. Any other officer who communicates with the media without being authorized to do so or who leaks information/documents to the public or media shall be guilty of misconduct.

CHAPTER 7

7. Computer Security

- 7.1 All computer storage media (usually magnetic or optical), are documents in terms of the definition in the Protection of Information Act (Act 84 of 1982). These documents, when containing classified information, must be handled according to the document security standards as described in Chapter 4.
- 7.2 All personnel dealing with classified information including executive secretaries and other support personnel must undergo computer security training in addition, the Security Awareness of all personnel using computer must receive regular attention.
- 7.3 Against this background the following measures must be implemented:
- S: Essential backup of computer systems and data;
 - S: Physical security measures as prescribed;
 - S: Computer security responsibilities should be clearly established;
 - S: The allocation and use of passwords as prescribed;
 - S: All administrative buildings or buildings where classified information is stored in computers must have facilities where a backup of computer systems and data are stored;
- 7.4 Departments must develop their own IT security policies.
- 7.5 All breaches of security in the computer environment must be reported as soon as possible to the departmental security manager.
- 7.6 In cases of uncertainty regarding the implementation or appropriateness of security measures in the computer environment, the Chief Directorate Security of the NIA should be consulted through the department security managers.
- 7.7 Computer passwords must be treated as confidential and must not be exposed in any manner in a way that will compromise the confidentiality thereof.

CHAPTER 8

PHYSICAL SECURITY

8.1 General

- 8.1.1 The Heads of Departments and security managers acting on their behalf are responsible for implementing and managing physical security in their departments. Physical security, even after implementing physical measures for the safeguarding of buildings, premises, people, information and assets, primarily embodies the application and monitoring of procedures. Heads of Department and security managers acting on their behalf are therefore responsible for the issuing of security measures and procedures to abide by and also to issue instructions to the personnel of the different institutions of that department, to co-operate with the security measures and procedures.
- 8.1.2 The level of physical security required at a specific office will be determined by a number of factors such as the crime rate in the area and the present existence of physical security measures (electronic and other).
- 8.1.3 Where more than one departments are sharing a building, it is the responsibility of the department which owns, control or occupies the most part of the building to install the necessary security equipment mentioned in this policy.

8.2 In cases of departments who are renting sections of a building belonging to a private company, such departments must, when they enter into lease agreements or renew such agreements, have included in their contract a part that will deal with security matters raised in this policy. In this regard it must be clear that the leaser will provide adequate security services. This includes access control, patrolling etc. The responsibility of the departmental security manager, having identified the needs of the department, will be to make his/her input to the contract being negotiated.

8.3 Access Control

- 8.3.1 The authority for the application of access control measures is derived from the Control of Access to Public Premises and Vehicle Act, 1985 (Act 53 of 1985). Security personnel are primarily responsible for the execution of access control and are therefore departmentally adequate to be subject to training programmes, which includes the application of the fore-mentioned and other relevant legislation.
- 8.3.2 Heads of Departments are responsible for the enforcement of the Control of Access to Public Premises and Vehicle Act (Act 53 of 1985) in their respective departments. They must issue instructions to the Heads of all institutions in their departments to enforce the same at their respective institutions for the purpose of safeguarding building or premises occupied, used or under the control of the department/institution.
- 8.3.3 Notices to the effect that the Act regarding the Control of Access to Public Premises and Vehicles is applied at the respective Municipality site(s) used by the Municipality, must be displayed at strategic places to inform members of the public who wish to gain access to some buildings or sites thereof.

- 8.3.4 Physical searching of persons by security personnel may only be conducted under certain conditions and Managers must give the necessary guidelines regarding searching in accordance with Control of Access to Public Premises and Vehicle Act, 1985 (Act 53 of 1985) read with Government Gazette Notice 1094 of 24 may 1991,. The Criminal Procedure Act, 1977 (Act 51 of 1977) as amended, and the Trespassing Act, 1959 (Act 6 of 1959).
- 8.3.4.1 In this regard, searching of persons at exits can only be executed by requesting a person to subject him/herself to it on a voluntary basis in accordance with the Act. The consent of the person to be searched, is thus an indispensable requirement. Where a person sought to be searched refuses to co-operate and there is reasonable suspicion on the side of security officer that the person possesses any item which is illegal or has an intention of entering the building with the intention of committing a crime, such a person may be denied access until searched by members of SAPS.
- 8.3.5 Searching of hand baggage and vehicles at exits should be executed on a random basis.
- 8.3.6 Access for the public to buildings must be controlled, and preferably only one route of access should be made available.
- 8.3.7 Visitor's registers must be implemented at all municipal sites and buildings and record must be kept of all members of public entering municipal buildings/premises.
- 8.3.8 Access may only be granted to persons with a valid reason to be on those premises.
- 8.3.9 Access must also be restricted to the specific area/office where the civilian needs to be to conduct his/her business.
- 8.3.10 Managers who do not have the services of security personnel, can appoint a member of staff to perform access control.
- 8.3.11 Visitors may not be left alone in offices. Heads of Office must obtain the co-operation of Heads of other institutions or tenants that may share the complex, in this regard.
- 8.3.12 Apart from the exceptions mentioned below no person (personnel included) may have a firearm or a dangerous weapon in his/her possession in a building or office or on premises occupied by the Municipality. In cases where people live in their places of work, firearms must be kept in accordance with the relevant law.
- 8.3.13 In terms of the Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985) paragraphs above and below are not applicable to a member of the South African Police Service or South African National Defense Force entering a building of the KwaZulu-Natal Provincial Government in the execution of his/her duties.

8.3.14 Firearms and dangerous weapons must be handed in at the access control point for safekeeping before access can be granted. In a person refuses to hand in a firearm or a dangerous weapon, access must be denied. However, this excludes close protectors to ministers or such protectors allocated to senior staff members of staff.

8.3.15 Security personnel must not handle the firearms themselves but must acknowledge receipt after it is locked away by the owner/bearer. The handing back of firearms taken in must equally not be handled by security personnel, but must be taken out of the firearm safes by the owners/bearers themselves.

8.3.16 Heads of Office who do not have the services of security personnel may appoint a member of staff to see to the locking away of firearms in the possession of any person who needs to enter the building/premises, in the firearm safes, with the exception as mentioned in paragraph 15 above. Notices to the effect must be displayed that no guns are allowed on the premises.

8.4 **Patrol**

8.4.1 It is absolutely necessary that patrol be conducted in and outside the building from time to time. In this regard, managers must develop patrol guidelines which will be based on such issues as the nature of the building, the nature of sensitive information being held and the high risk areas in the building. Such guidelines must make provision for regular patrols in all the floors in the building day and night. Observations made during such patrols must be entered in a register which must be inspected by a manager on weekly basis.

8.5 **Key Control**

8.5.1 Managers in departments must develop key control guidelines which will include control over duplicate keys, keeping of effective records, custody of safe/strongroom keys and the use of combination locks.

8.6 **High Risk Areas within Buildings**

8.6.1 Department security managers must identify in each and every building under their control, the high risk areas, which need special attention, e.g. Councillor Offices and areas where sensitive information is stored, e.g. matric examination papers. Once such areas have been identified, security managers must come up with a plan to be presented yearly to the HOD on how such areas will be protected. Depending on the risk involved, protective measures to be covered in such a plan can include such measures as:

- Assignment of permanent personnel to man entrances in such high risk areas;
- Installation of CCTV equipment;
- Installation of any other security equipment that might be necessary;
- Double locking system..

8.7 **Prescripts in Respect of Firearms**

8.7.1 The licensing and issuing of official firearms are dealt with in terms of section 45 of the Weapons and Ammunition Act, 1969 (Act 75 of 1969(m as amended and the Policy document on the Control of Government Owned Arms and Ammunition.

8.8 **Security Contracts with Private Security Contractors**

8.8.1.1 Security contracts as mentioned above, may be entered into when the need arises.

8.8.1.2 Certain requirements must, however, be complied with, namely:

8.8.1.3 **Need Assessments**

8.8.1.4 Departments are responsible to establish the need for private security services on their premises.

8.8.1.5 For this purpose, Departments should request their security administration components to conduct a security evaluation on site, in order to determine this need.

8.8.1.6 After the needs assessment, the security advisors must calculate and estimate cost. If this cost estimate exceeds the current budget of the department, the need must be adjusted, in collaboration with the security advisors, in order to be in line with the budget.

8.8.1.7 The availability of funds must be furnished in writing before any arrangements for the entering into contract can proceed.

8.8.2 **Requesting for Tenders**

8.8.2.1 When a department develops a need for a security contract appropriate tender procedures must be followed.

8.9 **Guarding and Training**

The following prescripts will apply for the offices that make use of the services of in-house security personnel.

8.9.1.1 Security personnel are appointed to perform protection services;

8.9.1.2 Security personnel may under no circumstances be utilized for purpose other than security tasks, which involves the following:

- Access Control
- Patrol duties
- Guarding duties
- Escort duties (visitors, cash and valuables)
- Security administrative
- Investigations

8.9.1.3 All administrative municipal buildings must have at their main entrances detector/x-ray machines installed or security officers with hand-held metal detector machines. These machines must be inspected by a department security manager or his/her delegate at least once a month. In this regard, the manager must satisfy him/herself that:

- The machine is in a good working condition
- Security personnel are making use of the detector/x-ray machine in accordance with the standard guidelines.

8.9.1.4 In cases where it is not practical and absolutely necessary to install the detector machines, the head of the department may make a decision that this requirement be dispensed with.

8.9.1.5 All departmental managers must ensure that they develop in their departments:

- (a) Guidelines for handling visitors entering the building/s, interacting with them and effecting a search and also for making use of detector/x-ray machines. The guidelines must also cover the issue of escorting visitors and the responsibilities of the members of staff/sections being visited. Such guidelines must be in line with the relevant legislation.
- (b) They must ensure that all security personnel undergo training on operating the detector/x-ray machines.

8.10 The following equipment should be provided/made available to assist the security personnel in the execution of their duties:

- 8.10.1 Hand held metal detectors
- 8.10.2 Two-way radios
- 8.10.3 Batons
- 8.10.4 Handcuffs
- 8.10.5 Torches
- 8.10.6 Whistles
- 8.10.7 Case register, occurrence book, exhibit register, pocket books and daily duty sheets
- 8.10.8 Visitors register
- 8.10.9 Control sheet
- 8.10.10 Gate control sheet for official and personal vehicles
- 8.10.11 Vehicle inspection form

8.11 The offices of on-duty security officers must be located within a fire meter radius from the location manned, e.g. entry point. The offices must be of the size that is conducive to the effective performance of their duties. Towards the above ends, the offices must be fitted with the following tools:

- A room wherein suspects could be searched in a dignified manner
- Gun safes
- Parcel racks
- A desk
- Veranda
- Proper lighting inside and outside

- 8.12 Application of these equipment will vary according to circumstances at each office and it is the responsibility of Heads of Office to procure and maintain the necessary equipment.
- 8.13 In-house security personnel must be provided with uniforms. For the purpose of uniformity and cost effectiveness, a standardized uniform should be implemented.
- 8.14 Departmental Managers and staff dealing with security matters must undergo the prescribed NIA training modules.
- 8.15 Departmental Managers will take the initiative in nominating personnel for formal training (prescribed courses). The specific tasks of security personnel are dealt with in the appropriate prescribed courses. The Security Officers/Guards as well as personnel dealing with security must be trained to the appropriate level in their occupation. The Manager must ensure that each Security Officer/Guard is subjected to the prescribed training programmes/courses.
- 8.16 **Office Security**
- 8.16.1 Each official in the Municipality is responsible for the securing of his/her office apart from the security measures as already mentioned in this directive.
- 8.16.2 If classified information and/or expensive equipment are kept or utilized in an office, the door must always be locked when the occupant leaves such office.
- 8.16.3 The cleaning of offices must at all times take place under supervision with the occupant or another trustworthy employee present.
- 8.16.4 Electrical appliances must be switched off before leaving the office at the end of the day.
- 8.16.5 In the event of an internal rotation or moves to other buildings, occupation must hand they keys of the previous office (and the access control card where applicable) to the key control officer.
- 8.16.6 It is the responsibility of each official to report any suspect items and/or person(s) to the most senior security official of that site. Apart from the aforementioned, if an item is suspected of being an explosive device, the SAPS and the Head of Office must be informed immediately.
- 8.16.7 Visitors must not be left alone in offices and when a visitor has to go to other staff members in the same building, he/she must be escorted to the specific location(s) office(s) as both a matter of courtesy and from a security perspective.
- 8.17 **Open Plan Offices**
- 8.17.1 All personnel employed by departments at some stage deal with information which need to be protected. The security of the information and the amount of protection required differs from section to section. Such information may be kept/stored in computers, filing cabinet, drawers and in some cases desk trays. It is therefore absolutely necessary that working conditions be created where not only information but also government assets can be protected.

8.17.2 It is therefore the responsibility of all departments to provide its employees with offices which cannot be accessed without the authority of the person who occupies it.

8.17.3 Toward the above end, open plan offices must only exist where it is not feasible to accommodate personnel in lockable offices. In such cases the following guidelines must be followed:

S: Staff dealing with sensitive information, whether classified or not must not work in open plan offices This include personnel dealing with personnel records, examination records, finances, etc.

S: Where it is not possible to locate personnel dealing with sensitive information in closed offices, such open space must be partitioned in a manner that reduces the security risk and must be locked.

8.18 **Smoking**

8.18.1 Each department shall develop a detailed smoking policy, however, the internal arrangement should be made to accommodate the right of smokers and non-smokers. Smoking is not be permitted in common areas like lifts, toilets, corridors, conference rooms, etc. Any employee who breach this policy will be dealt with in terms of disciplinary procedure on misconduct for acting against a departmental policy and endangering safety guidelines, rules or policy.

8.19 **Personal Belongings**

8.19.1 The Municipality is not responsible for the safeguarding of personal belongings. Managers should therefore inform their personnel to maintain the following precautions:

8.19.1.1 If more than one staff member occupy an office, or in the event of an open plan office, valuable items (personal as well as state owned) must not be left lying around unattended, but should be locked away.

8.19.1.2 Staff members with authorised parking in the premises should lock their vehicles and not leave valuable items, conspicuously in the vehicle.

8.19.2 Irrespective of the availability of security personnel, all Managers must assign staff members to periodically inspect all passages and waiting areas for strange (out of place) objects, bags and parcels. These staff members must also inspect toilets (cisterns) tea kitchens, tearooms and rooms where personnel are not always present.

8.19.3 All offices of personnel must be locked, even for short periods, when unoccupied.

8.20 **Parking**

8.20.1 Parking and access to the premises are subject to the Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985).

8.20.2 No vehicle must be permitted entry to a premises without the written/oral permission of the Head of the Office, which must at all times be displayed on the windscreen of the authorized vehicle.

8.20.3 No member of staff is automatically entitled to parking space. Parking is at all time subject to authorization by the Head of the Office, as well as the prescriptions that can from time to time be amended.

5.20.4 Unauthorized vehicles must not be parked against buildings and especially not next to offices of personnel.

8.21

Contingency Planning

8.21.1 Provision must be made for contingency planning aimed at preventing and/or combating any disaster or emergency. The contingency plan must be geared for saving lives, safeguarding property and information and ensuring that activities can continue with as little disruption as possible.

8.21.2 These aims can be achieved only through well-organized action in which all available means and manpower are used in a co-ordinated and effective way to put preventative and/or control measures into operation, and through regular practice of the contingency plan.

8.21.3 One of the purposes of a contingency plan is to ensure that every staff member know how to act in the event of an emergency. It is therefore necessary that information sessions should be held on a regular basis to keep staff updated with the contingency plan.

8.21.4 In this regard, all departmental managers must develop and manage contingency plans which must be reviewed on a yearly basis. This plan must cover the following:

- Emergency teams and their functions
- Evacuation plans
- Names and residential telephone numbers of the members of the control group, the action leaders, members of emergency teams, as well as reserves
- Telephone numbers of emergency services (fire brigade, ambulance, etc.)

8.21.5 All staff members must know where the contingency plan is kept.

8.22

Breaches of Security

8.22.1 This document constitutes a Municipal policy and is binding to all departments and staff. Failure to abide by the provisions of this policy constitutes a misconduct and the breach of security. Such misconduct must be dealt with in terms of rules and regulations governing the civil services.

- 8.22.2 Managers or those tasked with the security responsibility must report all instances of a breach of security, or failure to comply with security measures, or conduct constituting a security risk, as soon as possible to the Chief Directorate security of the national Intelligence Agency, and where appropriate to the SAPS (Crime Prevention Unit) or the SANDF (MI). Where official encryption is concerned, a security a security breach must also be reported to the South Africa Communication Security Agency (SACSA).
- 8.22.3 When a breach of security occurs, the exiting channels must be used to report it. It is the responsibility of the head of the institution to ensure that all breaches of security are reported.
- 8.22.4 A breach of the departmental policy on administration, discipline or efficiency of a department, office or institution of the State is misconduct and it shall be dealt with in terms of the public service rules and regulations and all the applicable labour laws. A guideline will be issued on how to handle such a matter in terms of this policy.

BIBLIOGRAPHY

1. Minimum Information Security Standards (MISS) document as approved by the Cabinet on 4 December 1996
2. The Security Policy for the Provincial Government of the Western Cape

RESTRICTED

SUGGESTED STRUCTURE: SECURITY POLICY

1. Introduction, Purpose and Scope
2. Statutory Requirements
 - Applicable acts and directives
 - Summary of applicable acts, regulations and directives
 - Implementation of statutory and other requirements
 - Structuring the security organization
3. Definitions
4. Responsibility for the Establishment and Implementation of Security Measures
 - 4.1 Structure
 - Security administration
 - Functional component
 - 4.2 Functions and Delegated Authority
 - Security administration
 - Functional component
5. Security Procedures
 - 5.1 Document security
 - Classification and reclassification of documents
 - Access to classified documents
 - Handling of classified documents
 - Transmitting documents by means of facsimiles
 - Transmitting documents by computer (e-mail)
 - Dispatching classified documents by courier
 - Dispatching classified documents by mail
 - Sealing of classified documents before dispatch
 - Bulk conveyance of classified documents
 - Storage of classified documents
 - Registries and files
 - Removal of classified documents from premises
 - The typing of classified documents
 - Making photocopies of classified documents
 - The handling of restricted documents
 - Contingency planning

5.2 Personnel Security

5.2.1 Vetting

- Introduction
- Vetting criteria
- Security screening in respect of immigrants and persons with more than one citizenship
- Screening/vetting of persons who have lived/worked abroad for long periods
- Security screening: contractors
- Procedure for requesting security screenings
- Period of validity of security clearances
- Transferability of clearances
- Responsibilities of the screening authority
- Responsibilities of the Head of the requesting institution
- Officers travelling abroad
- Protection of Executive officials

5.2.2 Security Awareness

- Introduction
- Inspections
- Programs

5.3 Community Security

- Voice encryption
- Fax encryption
- Cellular phones
- Board rooms and conference facilities

5.4 Computer Security

- Hardware security
- Network security
- Internet
- File encryption

5.5 Physical security measures

- Appraisal of physical security
- Access control
- Monitoring procedures
- Patrol procedures
- Fire control and detection
- Key control and combination locks
- Maintenance services, repairs and the cleaning of buildings/offices
- Contingency planning
- Firearm control

5.6 Breaches of security

- Reporting procedure
- Investigation procedures

6. Financial Aspects

- Introduction
- Operational expenditure
- Capital expenditure

7. Training

- Training of security personnel
- Training of security administration officials
- Training aids