SECTION ONE

1.1 PURPOSE

The Security Policy set out the fundamental responsibilities and security programmes for the Security Management in Fezile Dabi District Municipality. The Security Policy is the directive or guideline which is informed by Minimum Information Security Standards (MISS) document and outlines the formulation, implementation and effective monitoring of security measures in the Municipality and complies fully with the provisions of the MISS.

1.2 SCOPE OF THE POLICY

The Security Policy will cover the following categories:

2.1 Personnel Security

2.2 Document Security

2.3 Communication Security

2.4 Information Technology (IT) Security

2.5 Physical Security

2.6 Key Control / Management

2.7 Contingency Plan

2.8 Investigation of Security breaches

1.3 LEGISLATIVE FRAMEWORK

This policy must be read inter alia with the following documents:

- The Constitution of the Republic of South Africa (Act 108 of 1996)
- Municipal Structures (Act 117 of 1998)
- Municipal Systems Act 2002
- Control of Access to Public Premises and Vehicle Act (Act 53 of 1985)
- The Protection of Information Act (Act 84 of 1982)

- Protected Disclosure Act (Act 26 of 2000)
- The Promotion of Access to Information Act (Act 2 of 2000)
- The National Archives of South Africa Act (Act 43 of 1996)
- Firearms Control Act (Act 60 of 2000)
- The Public Service Act (Act of 1994)
- The Municipal Finance Management Act (Act 1 of 2002)
- The Criminal Procedure Act (Act 51 of 1977)
- The Trespass Act (Act 6 of 1959)
- Minimum Information Security Standards (MISS)
- Organisational Policies and Procedures (Fezile Dabi District Municipality)
- National Strategic Intelligence Act (Act 39 of 1994)
- Electronic Communication and Transaction (ETC) /Act (Act 25 of 2002)
- State Information Technology Act (Act 88 of 1988)
- Occupational Health and Safety Act (Act 85 1993)
- Private Security Industry Regulatory Act (Act 56 of 2001)

1.4 DEFINITION OF TERMS

1.4.1 Access Control

The process by which access to a particular area is controlled or restricted to authorised personnel only. This is synonymous with controlled access.

1.4.2 After Hours

For the purpose of this policy, after hours refers to-

(a) The time between 16:15 – 07:00
(b) Saturdays and Sundays; and
(c) Public holidays.

1.4.3 Author

The Municipal Manager, or the person acting on his/her behalf that prepares, generates, or initially classifies a document or has it classified.

1.4.4 Classification

The grading/ arrangement or re-grading/ re-arrangement of a document, in accordance with its sensitivity or in compliance with a security requirement.

All official matters requiring the application of security measures (exempted from disclosure) must be classified:

(a) **Confidential** relates to all information that may be used by malicious /opposing/hostile elements to harm the objectives and functions of an individual / or institution

(b) **Secret** relates to all information that may be used by malicious/opposing/ hostile elements to disrupt the objectives and functions of the institution and or state.

(c) **Top Secret** relates to all information that may be used by malicious/opposing/ hostile elements to neutralise the objectives and functions of the institution and or state.

1.4.5 Contingency Planning

The prior planning of any action that has the purpose to prevent, and or combat, or counteract the effect and results of an emergency situation where lives, property or information are threatened. This includes compiling, approving and distributing a formal written plan, and the practise thereof, in order to identify and rectify gaps in the plan, and to familiarise personnel and co-ordinators with the plan.

1.4.6 Compromise

The unauthorised disclosure/ exposure or loss of sensitive/ classified information, or exposure of sensitive operations, people or place, whether by design or through negligence.

1.4.7 Computer Security

That condition created in a computer environment by the conscious provision and application of security measures. This includes information concerning the procedure for procurement and protection of equipment.

Everything that could influence the confidentiality of data (an individual may have access only to that data to which he/she is supposed to), the integrity of data (data must not be tampered with and nobody may pose as another- for example in the electronic mail environment, etc) and or the availability of systems is considered to be relevant to computer security.

1.4.8 Communication Security

The conscious provision and application of security measures for the protection of classified/ sensitive communication.

1.4.9 Declaration of Secrecy

An undertaking given by a person who will have, has or has had access to classified/ sensitive information, that he/she will treat such information as secret.

1.4.10 Delegation

Delegation is the transfer of authority, powers or functions from one person/ department to another. Delegation takes place in order to effect division of labour since it is physically impossible for a person/department/body himself/herself to exercise all the powers/ authorities assigned to him/her.

1.4.11 Destruction of classified material

Expunging or destroying of classified/sensitive documents.

1.4.12 Director

A person appointed in terms of section 57 of Municipal Systems Act

1.4.13 Document

In terms of the Protection of Information Act (Act 84 of 1982), a document is any note or writing, whether produced by hand or by printing, typewriting or any other similar process, any copy, plan, sketch or photographic or other representation of any place or article or any disc, tape, card, perforated roll or other device, in, or on which sound or any signal has been recorded for reproduction.

1.4.14 Document Security

The conscious provision and application of security measures in order to protect classified/ sensitive documents.

1.4.15 Employees

For the purpose of this policy the term employees includes:

- Permanent staff;
- Temporary/contract staff;
- Seconded employees; and
- Contractors that are employed by Fezile Dabi District Municipality;
- Consultants.

1.4.16 Espionage

The methods by which states, organisations and individuals, attempt to obtain classified information to which they are not entitled.

1.4.17 Executive Mayor

An Executive mayor elected in terms of section 55 of Municipal Structures Act

1.4.18 Host

An employee of the instituition who receives or entertains another person or member of the public as guest.

1.4.19 Information Security

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

1.4.20 Municipal Manager

A person appointed in terms of section 82 of Municipal Structures Act

1.4.21 Need to know principle

The furnishing of only that classified information or part thereof that will enable a person/s to carry out his/her task.

1.4.22 NIA – National Intelligence Agency

1.4.23 Personnel security

Personnel security is that condition created by the conscious provision and application of security measure in order to ensure that any person who gains access to sensitive/classified information has the necessary security clearance, and conducts himself/herself in a manner not exposing him/her or the information to compromise. This could include mechanisms to effectively manage/solve personnel grievances.

1.4.24 Physical security

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

1.4.25 Premises

For the purpose of this policy, premises shall refer to any building, structure, hall, room, office, land, enclosure or water surface which is the property of, or is occupied by, or is under the control of Fezile Dabi District Municipality and to which a member of the public has a right of access.

1.4.26 SANDF- South African National Defence Force

1.4.27 SAPS- South African Police Service

1.4.28 SASS- South African Secret Service

1.4.29 Screening/Vetting Institution

Screening institution are those institutions (the SAPS, NIA, SASS, and SANDF) that, in terms of the rationalisation agreement, are responsible for the security screening/vetting of persons within their jurisdictions. NIA has a legal mandate to employees within the Public Service.

1.4.30 Security

Security is concerned with the provision and application of appropriate standards and measures intended to provide protection to people, property, information and other assets against the security risks and most threats to which they are exposed.

1.4.31 Security area

Any area to which the general public, and in some cases, certain employees are not freely admitted and to which only authorised persons are admitted.

1.4.32 Security audit

That part of security control undertaken to determine the general standard of information security and to make recommendations where shortcomings are identified, evaluate the effectiveness and application of security policy/standards/ procedures and to make recommendations for improvement where necessary; provide expert advice with regard to security problems experienced; and encourage a high standard of security awareness.

1.4.33 Security clearance

An official document that indicates the degree of security competence of a person.

1.4.34 Security competence

This is a person's ability to act in such a manner that he does not cause classified information or material to fall into unauthorised hands, thereby harming or endangering the security or interests of the State/Municipality. Security competence is normally measured against the following criteria: susceptibility to extortion or blackmail, amenability to bribes and susceptibility to being compromised due to compromising behaviour, and loyalty to the State/department.

1.4.35 Security measure

All actions, measures and means employed to achieve and ensure a condition of security commensurate with the prevailing treat.

1.4.36 Security Manager

The Security Manager bears overall responsibility for the provision and maintenance of security in all the buildings/ premises of the department, under all circumstances in terms of the Private Security Industry Regulatory Act (Act 56 of 2001). Moreover ensures the implementation of the Security policy of the Municipality.

1.4.37 Security Vetting

It is the systematic process of investigation undertaken to establish the security competence of an employee with the intention of protecting the State and its inhabitants from foreign intelligence services and corruption.

1.4.38 Sensitive/ classified information

Information, which in the national interest is held by, produced in, or is under the control of the department, or which concerns the Municipality and must, by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.

1.4.39 SM – Senior Management

1.4.40 Speaker

A Counsellor elected in terms of section 36 of Structures Act to be the chairperson of a Municipal council as envisaged in section 160 (1)(a) of the Constitution.

1.4.41 Storage

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

1.4.42 Transmission security

Transmission security is a part of communication security and entails the safeguarding and secure use of system linked to one another for the sake of communication.

1.4.43 Visitors

Non employees of Fezile Dabi District Municipality including any other person such as clients and contractors entering the premises.

1.4.44 Work Station

Security offices, stores, behind counter of cashier in finance, control room, registries, kitchens, photocopy rooms, library, etc

1.5 POLICY STATEMENT

The functional performance of the various security measures and procedures is primarily the responsibility of each and every employee of the Municipality, irrespective of rank. Each Component Head must ensure that all personnel, assets and information under his control are safe and secure at all times and that the relevant procedures are adhered to and that any discrepancies are reported timeously to the Security Manager.

1.6 SCOPE OF APPLICATION

The Security Policy shall be applicable to the internal stakeholders, that is, The Executive Mayor, The Speaker and Staff, The Municipal Manager, Senior Management, Employees, Service providers (contractors), Consultants and visitors.

No one will be exempted from any security measures or procedures as laid in the policy because exceptional treatment will reduce the effectiveness of the security system, create loopholes and/ or eventually cause the downfall of the security system.

Thus, Senior Management members and the management in general are expected to lead by example and will be held accountable if not complying with and implementing all the security procedures contained in this policy.

This policy will consider the ability of employees and visitors who are physically challenged and other considerations as the need arises.

1.7 ROLES AND RESPONSIBILITIES

1.7.1 Municipal Manager: Fezile Dabi District Municipality

In terms of Section 1 and 2 of the Control of access to Public Premises and Vehicle Act (Act 53 of 1985), Chapter 3 of the Minimum Information Security Standards (MISS) document of 1996 as well as the contextual interpretation of the Public Service Act of 1997 and Section 38(1)(a), the Municipal Finance Management Act (Act 1 of 2003 as amended), Municipal Structures Act (Act 117 of 1998) Municipal Manager bears overall responsibility for the provision and maintenance of security in all the premises/building of the institution.

1.7.2 Security Manager

The Security Manager shall be responsible for the following:

1.7.2.1 Manage the total security function (personnel, document, physical,

communication, and computer security).

1.7.2.2 Draft internal security policy, based on the MISS document (national information security policy)

1.7.2.3 Advice Management about amendments to such a policy.

1.7.2.4 Advice Management about the security implications of Management decisions.

1.7.2.5 Identify all risk and threats to the security of the institution as well as vulnerabilities in the institution's capacity to counter these.

1.7.2.6 Devise all security measures and procedures for the whole Municipality based on the security policy.

1.7.2.7 Evaluate and improve the effectiveness of security measures and procedures.

1.7.2.8 Create, develop and maintain a security training capacity to the Municipality and conduct security-training sessions of all officials.

1.7.2.9 Run a security awareness program in the Municipality

1.7.2.10 Monitor the extent of adherence/compliance to the security policy and measures, including the vetting of officials with access to sensitive information.

1.7.2.11 Liaise regularly with NIA for advice, assistance and information regarding information security.

1.7.2.12 Report to NIA all incidents or suspected incidents of security breaches and/or leakages of sensitive information, for investigation. Keep records of all incidents (e.g. leakages, thefts/burglaries, tampering with security systems, etc.

1.7.2.13 Liaise with the relevant authority on all physical security needs, problems, etc. to ensure effective security.

1.7.2.14 Ensure the effective implementation of all security measures.

1.7.2.15 Ensure the proper administration of vetting applications. This includes the keeping of records of all posts that require security clearances in the Municipality, ensuring the completeness of vetting applications before submission to vetting institution.

1.7.2.16 Establish and chair the Security Committee comprising of representative from all components (business units) in the Municipality.

1.7.2.17 Co-ordinate the Safety and Security of the MECs within the entire District.

1.7.2.18 Co-ordinate Security Managers within the Fezile Dabi District Municipality with regard to the implementation of their Security Policies And other matters related to Security.

1.7.3 SECURITY COMPONENT

The Security Component is responsible for the control and co-ordination of all security matters in the institution. It must ensure that policies, procedures and standards are maintained throughout the institution and must promote dissemination of instructions and efficient reporting of incidents to the relevant heads of departments.

1.7.3.1 The following main activities are executed by the SC:-

1.7.3.1.1 The overall supervision of the entire security function and security personnel within the institution

1.7.3.1.2 On an ongoing basis do research, studies, inspections and investigations pertaining to all aspect of security;

1.7.3.1.3 Effectively liaise with other institutions in connection with all security matters and where necessary render advise and support;

1.7.3.1.4 Drawing up and continuously updating the policy guidelines with respect to the different facets of security;

1.7.3.1.5 Catering for training needs of the Municipality through instituting, supplying and arranging seminars for orientating, motivating and training of all staff;

1.7.3.2 In order to achieve the above, the following must be performed:-

- Effective access control must be enforced;
- Building and sites must be regularly inspected and continuously patrolled;
- Supervision of cleaning and maintenance personnel with a view to security;
- All aspects of the security, fire and emergency systems must be monitored;
- All shortcomings must be reported to NIA;
- Incidents of crime must also be reported to SAPS
- Maintaining contact with all institutions in order to ensure a more holistic approach to combating crime and securing of government assets.

1.7.3.3 The outsourcing of services relating to security, is the task of SC and the component must ensure that:

- Sites, installations and stands are identified according to the directives as laid down, for possible outsourcing;
- Conditions, specifications and contracts/tenders with respect to the outsourcing of such services;
- It adjudicates and make recommendations on the awarding of a specific contract/tender;
- Inspection of services that are rendered by contract companies.

1.7.4 EXECUTIVE MAYOR, SPEAKER, MAYORAL COMMITTEE MEMBERS, MUNICIPAL MANAGER, DIRECTORS, MANAGERS AND EMPLOYEES

1.7.4.1 An effective security measure requires a careful thought, cooperation and concern from all politicians and employees. The support of all employees is indispensable to control security breaches and losses at the workplace. Proper security refers to the combination of all security measures including the officials' and politicians joint efforts. All politicians and officials should join hands in realising the safeguarding of council`s property and information

1.7.4.2 Employees' support is deemed to consist of willing co-operation in all anti-loss systems and an awareness of the need for security.

1.7.4.3 All the politicians and employees of Fezile Dabi District Municipality are expected to do the following contributions;

- Adhering to the "clean desk policy" as adopted by the institution;
- Locking away valuable assets and sensitive documents in cabinets' when not in use;
- Securing their workstations/office layout and restricting access/entrance;
- Disposing of classified/sensitive papers in an appropriate manner (shredding);
- Not storing or saving sensitive/classified information on laptops;
- Reporting suspicious visitors to security;
- Reporting suspected security breaches (e.g. theft); and
- Looking after their keys and ensuring that such keys do not fall into the wrong hands.

1.7.4.4 Effective access control should be applied to areas where photocopiers, printers, fax machines, etc., are used. Municipal Manager, Directors, Managers must keep this equipment under constant supervision to ensure that no unauthorised transmissions of classified/ sensitive documents take place or unauthorized copies are made.

1.7.4.5 All employees at all levels are expected to play an important role in ensuring that personnel, assets and information of the department are safe and secure.

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

1.7.4.7 Directors and Managers are responsible for the implementation of all security measures within their components, floor/blocks and units. The Directors represents their respective components in ensuring the implementation of security measures. This is applicable to all Fezile Dabi District Municipality buildings.

1.7.5 SECURITY COMMITTEE

The Security Committee shall be established and comprise of representatives from all components (business units) of the Municipality to carry out the following functions: [The Security Manager shall be the chairperson of the committee]

1.7.5.1 Identify categories of information that require protection

1.7.5.2 Identify which components in the Municipality handles such information

1.7.5.3 Identify who may require access to such information (internal/ external)

1.7.5.4 Identify the physical area where the information is handled or stored

1.7.5.5 Identify history of security breaches with regard to information

1.7.5.6 Consult with NIA to identify trends with regard to the compromise of information

1.7.5.7 Assist the Security Manager with conducting of Treat and Risk Assessment

1.7.5.8 Assist the Security Manager with the drafting and reviewing of the security policy, plan and procedures

1.7.5.9 Assist in awareness program

SECTION TWO

"2 PERSONNEL SECURITY

Aim : To describe the minimum security measures that shall be implemented to reduce the risk of human error and to prevent the personnel and contractors from committing sabotage, espionage, subversion or actions posing the security threat.

2.1 SECURITY CHECKS

(a) All prospective employees shall be subjected to security checks when they take appointments up with the Fezile Dabi District Municipality. When security checks are favourable, the prospective employee will be employed on probation, during which proper vetting will be conducted.

(b) The permanent appointment of the prospective employee will depend on the outcome of the results of proper vetting.

2.2 SECURITY VETTING

(a) The main focus of the security vetting process is to determine the integrity, reliability and loyalty of an official towards the Republic of South Africa and the Constitution.

(b) This must be regarded as the basic defence measure that can be taken to protect classified and sensitive information.

(c) The degree of security clearance given to an employee is determined by the content of and/ or access to classified information entailed by the post already occupied/ to be occupied by the official.

(d) In terms of the policy vetting authority (NIA), there are three categories of security clearance, that is, confidential, secret, and top secret.

(i) **Confidential** – This category is for employees who have access to information that can harm the objectives and functions of an individual and or institution if such information is leaked to malicious/ opposing/ hostile elements.

(ii) **Secret**- This category is for employees who have access to sensitive/ classified information that can result in disruption of the objectives and functions of the institution if such information is leaked to malicious/ opposing/ hostile elements.

(iii) **Top Secret**- This category is for employees who have access to sensitive/ classified information that can result in the neutralisation of the objectives and functions of the institution and or State if such information is leaked to malicious/ opposing/ hostile elements.

(e) Political appointees, that is the Municipal Manager, Directors need to be vetted because they will be having access to classified information. This means that they must have the security clearance to the level of Top Secret. Other Officials will be vetted up to the level of Secret depending on the nature of their specific jobs. The Security component will be must be cleared up to the level of Top Secret due to the nature of their job.

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

2.3 VETTING CRITERIA

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

2.4 SCREENING OF APPLICANTS WHO HAS LIVED / WORKED ABROAD FOR LONG PERIODS, OFFICIALS MORE THAN ONE CITIZENSHIP AND FOREIGN NATIONALS

(a) Where a security clearance is required for RSA citizen who has resided/ studied/ worked abroad for longer period (excluding transferred public servants or students) and who applies for a position in the Municipality, such a person is temporarily not eligible for any grade of security clearance. Applications for clearance can, however, be considered after a period, as spelled hereunder, on condition that the applicant did not give up RSA citizenship or accepted dual citizenship during the period of absence.

(b) A confidential clearance may be granted 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 Fezile Dabi District Municipality will inform the National Intelligence Agency 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 undertaking is not

specifically included in the service contract, a written undertaking to this effect, under signature of the subject, must accompany the application for a security clearance.

(c) Security clearance of officials who have lived/ worked/ studied abroad for long periods, officials with more than one citizenship and foreign nationals shall be handled as follows:

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

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

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

(iv) Dual Citizenship. According to MISS Chapter 5, Par 3, each application for a security clearance in respect of persons with dual citizenship will be assessed on the merits of each individual case. No clearance can be issued in the following cases:

- Persons without valid identification documents.
- Any person who is not in possession of a valid identification document or residence permit for the RSA
- Naturalised RSA citizens who have not applied for a new identification document after naturalisation, since the document that was issued before naturalisation expires on naturalisation.

2.5 EMPLOYEES WHO DO NOT MEET SECURITY- SCREENING STANDARDS

In the case of an official who has lived/ worked/ studied abroad for long periods, official with more than one citizenship, a foreign or a national who does not meet the security clearance requirements, the following must be adhered to:

(a) If on account of the indispensable expertise of the official, it is considered to be essential to employ him/her, the Municipal Manager must make a decision to employ the official.

(b) A certificate must be submitted to the National Intelligence Agency 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;

(c) Provide the National Intelligence Agency with a description of, and an indication of the sensitivity of the responsibilities attached to the post to be occupied by the immigrant;

(d) The official must declare that he/she accepts full responsibility for compliance with the security requirements connected with the employment of such immigrant;

(e) The Municipal Manager must ensure that no classified information or material that is not needed for the performance of his/her duties comes into the Possession of the incumbent; and

(f) Reconsider the authorisation 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 incidences which may bring his/her security competence into question.

(g) When the person concerned changes his/her posting, the authorisation is automatically terminated.

(h) In respect of an immigrant already employed in a sensitive position and in whose case the conditions laid out in paragraph 2.4.(c)(iv) referred to above, have not yet been complied with, the employing institution must immediately give effect to those conditions as set out in paragraph 2.4.(c)(iv) of the policy.

2.6 SECURITY SCREENING OF CONSULTANTS/CONTRACTORS ATTACHED TO THE FEZILE DABI DISTRICT MUNICIPALITY

(a) It is the onus of the Fezile Dabi District Municipality to expressly indicate in advance on the documents sent to the Tender Committee or private contractors the security implications that should be taken into account when they perform their duties for the Fezile Dabi Distrcit Municipality. A reason must be given for the inclusion of such 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 should read as follows:

- Acceptance of the tender is subject to the condition that both the contracting company and its personnel providing the service to the Fezile Dabi District Municipality, must be subjected to record checking as an interim measure before they can be cleared by the National Intelligence Agency to the level of CONFIDENTIAL/ SECRET/ TOP SECRET. If the principal contractor appoints a subcontractor, the same provisions and measures will apply to the subcontractor subject to NIA vetting the contractors who are working with long term contractors i.e. 6 months and above and firms working sensitive information or sensitive areas.

(b) 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.

(c) The security responsibilities of the contractor must be determined by the Municipal Manager, the Security Manager, Procurement,Technical and Finance Directors who must advice directorates in this regard.

2.7 PROCEDURE FOR REQUESTING SECURITY SCREENINGS

(a) The responsible management shall inform and must provide the Director of Corporate Support Services with a job description of all new employees employed with an indication of the access to classified information that the employees have in their respective establishments. A completed and signed action of Secrecy Form(ANNEXURE A) must also be attached.

(b) All requests for vetting and/or re-vetting must be submitted to the municipal Manager for Security Manager's attention.

(c) A photo must accompany the requests on the security clearance form Z204 including a set of clear fingerprints, and a covering letter indicating the functions of the intended post, level of clearance, priority and any previous clearances.

(d) Re-screenings of security clearances should be done every five (5) years for Top Secret and Secret levels and every ten (10) years for confidential
level

(e) The screening authority in the case of the Fezile Dabi District Municipality is the National Intelligence Agency (NIA), who will investigate and advice on the security competence of an official on the basis of prescribed guidelines. The Municipality vetting unit shall be established to carry out field work/information only on the complementing NIA's capacity of ensuring efficient and effective vetting processes.

(f) After the investigation, the National Intelligence Agency will merely make recommendations regarding the security competence of the official concerned to the Municipal Manager.

(g) Upon receiving a positive recommendation from the NIA regarding a security clearance, the Municipal Manager will convey the information if the applicant is the Manager. In the case the applicant is the not the Manager the Security Manger will be responsible for the conveyance of the results of vetting from the vetting authority.

(h) Upon receiving a negative recommendation from the National Intelligence Agency regarding a clearance, the Municipal Manager may still, after careful consideration and with full responsibility, use the official concerned in a post where he/she has access to classified information, if he/she is of the opinion that the use of the official is essential in the interest of the Fezile Dabi District Municipality, on the understanding that the official satisfying the clearance requirements is not available. Otherwise the employee will be re-deployed.

2.8 TRANSFERABILITY OF CLEARANCES

(a) The security clearance is issued in respect of an official while attached to the Fezile Dabi District Municipality and will automatically be transferred to other departments within the institution. The Directors concerned will inform the Security Manager of the changes effected.

2.9 RESPONSIBILITY OF NATIONAL INTELLIGENCE AGENCY AS THE SCREENING AUTHORITY

(a) To conduct security screening investigations of any person who (except for SAPS, SASS and SANDF employees):
- is employed by or is an applicant to an organ of state; or

- is rendering a service or has given notice of intention to render a service to an organ of state, which service may
    - give him or her access to classified information and intelligence in the possession of the organ of state; or
    - give him or her access to areas designated national key points in terms of the National Key Points Act, 1980 (Act 102 of 1980).

(b) In performing the security screening investigation, NIA may use a polygraph to determine the reliability of information gathered during the investigation.

(c) For the purpose of this section, "polygraph" means an instrument used to ascertain, confirm or examine in a scientific manner the truthfulness of a statement made by a person.

(d) NIA may, in the prescribed manner, gather information relating to-
- criminal records;
- financial records;
- personal information; or
- any other information which is relevant to determine the security clearance of a person:

(e) Provided that where the gathering of information requires the interception and monitoring of the communication of such a person, the relevant members shall perform this function in accordance with the provisions of the Interception and Monitoring Prohibition Act,1992 (Act No. 127 of 1992)

(f) DG of NIA may, after evaluating the information gathered during the security screening investigation, issue, degrade, withdraw or refuse to grant a security clearance.

(g) DG of NIA may establish a security screening Advisory Board comprising of members or employees of NIA to assist him in the determination of the security competency of a person.

2.10 VISITS ABROAD

(a) In the event where an official with a clearance travels abroad, Secretary or the person assigned for the preparations must keep record of such visits. The appropriate form (Annexure B) must be completed and submitted to the Security Manager.

(b) 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 Municipal Manager, Security Manager and such information will be conveyed to the National Intelligence Agency. While travelling, officials must maintain a low profile and be careful not to place themselves under compromising situations.

(c) In the event the official receives gifts abroad, such gifts must be declared and forwarded to Security Manager for examination before being opened or used.

2.11 STATUTORY AND OTHER PROVISIONS FOR THE PROTECTION OF INFORMARTION

(a) The attention of all officials dealing with classified matters should be drawn specifically to the provisions of the Protection of Information Act (Act 84 of 1982) as amended, and promotion of Access to Information Act (Act 2 of 2000).

(b) The Municipal Manager and Directors need to bring any other legislation, regulations and/or directive relating to secrecy and/or the safeguarding of the information, activities, installations, etc. of the matters in the departments possession with which they are dealing, to their attention to ensure this is protected.

(c) The Municipal Manager and Directors will be informed in writing once a security clearance has been issued to an official in their components.

SECTION THREE

3 INFORMATION SECURITY

Classified information refers to information in possession of or produced by or in the control of Fezile Dabi District Municipality, or information in which the Municipality has interest and which because of its nature must be protected from unlawful revelation of publication.

3.1 Levels of classification of information/document

The Municipality intended to classify the information in the sensible way that is appropriate to the organisation;

- **Unclassified** - this level is considered publicly accessible. There is no requirements for access control or confidentiality.
- **Shared** - resources that are shared with groups or with people outside the organisation. This can include data that is legitimately accessed by outside people and the resources.
- **Institution only**- access to be restricted to the employees only not any other person, group or party.
- **Confidential** - access to be restricted to a specific list of people. For someone to have access to the resource classified as "CONFIDENTIAL" must be cleared at that level and be included in the list for this resource.

3.2 The handling of classified document

The Municipal Manager, Directors and Managers must ensure that the following aspects pertaining to the handling of classified documents are adhered to:

- All documents must be classified and re-classified correctly according to prescriptions;

- The prescribed classification is adhered to at all times.
- The "need to know" principle must be applied at all times in the distribution of classified information;
- The official to whom such sensitive information is given is correctly cleared
- The necessary provisions exist in registry for the dispatch and receipt of such documents; where the correct methods of sealing of such documents are required the necessary registers and systems of proof of receipt/dispatch must be adhered to;
- That such documents are supplied with numbers and that dispatch lists are retained so that the document or a copy thereof can be found;
- That such documents are not unnecessarily duplicated and where necessary, such duplications must be done by a properly cleared person and with the necessary indication on the original, of the number of copies made, and for whom;
- All such documents are removed from their place of safekeeping on the strength of written authority only;
- All such documents are typed only by properly cleared persons;
- The correct supervision is maintained with the destruction of all the typing-waste, (use of shredding machine is recommended);

- All Directorates, components or sections dealing with such information have the necessary safes and strong rooms to store all the classified information.

- Maintenance services, repairs and cleaning of offices should be carried out in the presence of the office occupant, and all classified documents should be locked away.

3.3Making photocopies of classified documents

All mechanical/electronic reproduction appliances should be properly controlled to prevent the unauthorised or uncontrolled copying of classified documents. (Photocopy register should be utilised for this purpose).

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.

3.4Communication Security

The Municipal Manager, Directors, Deputy Managers and Managers must take care and ensure that:
No classified information pertaining to communication apparatus is discussed/dispatched if they do not have the necessary crypto equipment;

- Where facsimile apparatus is used for the dispatch of classified information there is a register to record such information as in the case of photocopy machine;

- Classified information is not discussed in public places or revealed to the media;

- The staff does not indulge in careless talk about classified information and that clear guidelines are drawn up and disseminated to all staff with regards to discussing classified information with visitors.

3.5 Computer security

Computers in the administration of the Municipality and country in general, and also of the extent to which classified information is processed by means of computers, security has become essential.

All computer storage media 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 as stipulated above under the heading "Handling of classified documents".

Against this background the following measures must be implemented:-

- Essential backup of computer and data (use of discs);Physical security measures as prescribed;
- The allocation and use of passwords as prescribed (i.e. the locking of files using password)

Note : that the Information and Communication Technology Policy has been developed separately from this policy. In future both policies will be reviewed, consolidated to form one Security Policy.

3.6 Specific Employees Responsibilities

- Comply with legislation, National Security Standards and this policy, procedures and directives to protect information
- Sign a Declaration of Secrecy
- Report any changes in personal life that may be of security interest

- Report any information regarding known or suspected foreign intelligence activity directed against themselves, a co-worker, the Municipality , or the national interest

- Report any information that raises doubts about the reliability or trustworthiness of any co-worker or other person with access to classified or other protected information

- Understand the foreign and domestic threats that make these security measures necessary

- Failure to comply with responsibilities should be sanctioned by administrative action (security clearances and/or disciplinary measures)

- Deliberate violation for individual profit must be criminally prosecuted

- Protection of classified/sensitive information of Fezile Dabi District Municipality is a LIFELONG obligation

SECTION FOUR

4 PHYSICAL SECURITY PROCEDURES

Aim: To describe the minimum physical preventative, detection and corrective security measures which shall be implemented in the Municipality facility for protection against unauthorised access and damage to interference with information and/or information system.

The following security procedures are compulsory and must be adhered to by all employees:

4.1 PHYSICAL SECURITY MEASURES

4.1.1 Access Control

The under mentioned physical security procedures are developed to minimise vulnerability or to reduce the threats or risks faced by the Fezile Dabi District Municipality.

4.1.1.1 Employee Access Tags

(a) Access control will be applied in terms of the Control of Access to Public Premises and Vehicle Act, (Act 53 of 1985). The act stipulates the manner in which public premises and vehicles should be safeguarded and also the protection of people therein or thereon.

(b) No persons shall, without the permission of a Security Officer, enter any of the buildings occupied by the Fezile Dabi District Municipality.

(c) For the purpose of granting of that permission the Security Officer may request that the person concerned:

- furnish his/her name, address and any other relevant information required by the authorised officer;
- produce proof of his/her identity to the satisfaction of the authorised officer;
- declare whether he/she has any dangerous object in his possession or custody;
- declare the nature of the contents of any vehicle ,suitcase, attache' case, bag, handbag, folder, envelope, parcel or container of any

nature, which is in his/her possession or custody or under his/her control, and show those contents to the Security Officer;

- subject himself/herself and anything that he/she has in possession or custody or under his/her control to examination by an electronic or other apparatus in order to determine the presence of any dangerous object;

- hand to an authorised officer anything, that he/she has in his/her possession or custody or under his/her control for examination or custody until he/she leaves the premises or vehicle; and

- in the case of premises, or a vehicle or class of premises or vehicles determined by the Minister in the Government Gazette, be searched by an authorised officer.

(d) Entrances/ exits must be reduced to the absolute minimum (taking in to account the smooth/ effective operation of the Municipality in terms of congestion) to ensure the elimination of unnecessary access points, and the proper control of those remaining.

(e) The installed security system in all Fezile Dabi District Municipality buildings allows doors/ turnstiles at each point to be accessed with tag readers and biometric readers. A locking mechanism, fitted with a means for activating it, is installed in on the barrier. Access to the building occupied by the Executive Mayor and the Speaker will be granted when proper identification is made available either through the mechanism or Security Officer responsible.

(f) Private property brought into the premises must be declared and be entered into the security registers for asset audits and so that on departure no removal permit would be demanded by Security Officers as the property would be confirmed in the Private Property Register, which is kept at the Security Desk.

4.1.1.2 Exit Control and the Movement of Assets

(a) The purpose of access control is to safeguard public premises and vehicles and to protect the people therein. Exit control includes both electronic and physical searches. It is mainly aimed at or directed to theft prevention.

(b) Therefore, all vehicles (private or government owned) may be searched when leaving the building occupied by the Municipality. Property, equipment, parcels, documents, etc shall be taken out of the buildings with official removal permits signed by authorised official.

(c) The following people will be subjected to exit control:

(i) All Managers
(ii) All employees
(iii) Contractors; and
(iv) Visitors (general public and public servants from other departments).

All identified Very Important Persons (VIP's) and their crew/ team may be subjected to access and exit control procedures in exceptional cases.

4.1.1.3 Handling of Visitors

(a) Apart from the control of employees entering and leaving the premises, visitors must also be subjected to access control procedures.

(b) When a visitor arrives at the security main reception areas of the building the normal access control procedures will be applied. When the visit/ appointment is confirmed with the host, the security officer responsible will open and refer him/ her to the floor secretary/ host/ receptionist. The host shall ensure that the visitor displays the visitor's card visibly at all times while in building. Visitors found in the building shall be requested to produce their visitor's cards, failing which, they shall be requested to leave the building. Should they refuse to leave the building, the Trespasses Act 6 of 1959 shall be applied.

(c) All visitors entering the buildings of Fezile Dabi District Municipality shall use the main entrance and pass trough the designated reception for the necessary security checks, where also the normal access control procedures will be followed. All visitors shall park at the parking bays which are clearly marked and reserved for Visitors only.

(d) The host shall collect the visitor/s from the main reception and escort them back on departure. The security shall escort visitors to the host, only if the host is the Executive Mayor, the Speaker and Municipal Manager and Directors. The mentioned visitors will be escorted when a notice of their visit is prior registered with the Security Services.

(e) No visitors will be allowed in the work station/areas.

(f) After the meeting, the host will take the visitor back to the security main reception. The employee being visited shall ensure that his/her visitor does not wonder around the buildings. Visitors found loitering in the buildings shall be taken to the security services for questioning.

(g) All employees must co-operate in controlling the movements of strangers on the premises, either by reporting their presence or inquiring about the purpose of their visit and where no satisfactory account is given, the stranger must be reported to the security control rooms or receptions.

(h) When in the buildings, visitors should be accompanied by the host and restricted to the place visited.

(i) Control measures for visitors include:

(i) requiring visitors to report to the security counters/ receptions on their arrival and departure;

(ii) confirming appointment at the security counter/ reception with the host prior to access being permitted to the premises; and

(iii) completing a visitor's register after producing an identity document or appointment certificate in the case of the National Intelligence Agency, South African Police Service, National Prosecution Authority and the South African National Defence Force (only when visiting the premises in their official capacity).

4.1.1.4 After Hour Control

(a) Control of access after normal business hours will include electronic or manual recording of movements of all employees in and out of the premises of Fezile Dabi District Municipality.

(b) Employees will only be given access to areas where their offices are located and should they need to access other areas (including restricted areas) they must get permission from Security Manager.

(c) Contractors or temporary/ casual staff will not be given access to the premises unless an arrangement is made with the relevant Directors and the Security Manager is inform in that regard.

(d) All short term (i.e day to day) contractors working in the building shall be escorted by security officer(s) to the employee who arranged such work. The employee shall supervise and be responsible for the movements of the contractors while in the buildings and report any irregularity/ security breach to security services.

4.1.1.5 Key Control and Combination Locks

(a) Security Component has overall responsibility for effective control of all keys within the Municipality, all employees are responsible for

safeguarding them and prohibited from duplicating these keys. Directors and Managers must ensure that proper control is implemented. The Security Manager will advise the senior officials about the effective control of keys. Effective key control includes control over duplicate keys and keeping of effective records in order to ensure that the keys to the buildings, safes, strong rooms or other safe storage places, in which classified information is kept, are dealt with in a safe manner.

(b) Where storage places are equipped with combination locks, the combinations must be used, kept and changes in accordance of Chapter 3 (Par 2) of the MISS.

(c) The Municipal Manager shall, in writing, appoint a competent person to act as the main key custodian at a Senior Manager level of the institution. Senior Managers of directorates must appoint key control officers responsible for their directorates offices. The key control officers must report to the main key custodian on a quarterly basis.

(d) The appointment of a key and lock custodian is the most important step in ensuring the proper custody and handling of keys and locks. Duties of the key custodian must be clearly defined and include the following:

- Compiling of a locking system policy.
- Establishment of key control registers.
- Compiling of all routine letters and reports with regard to incidents and investigations.
- Compiling of monthly reports with regard to key control issues.
- Storing of the locks and keys.
- Managing of the keys.
- Maintain of records with regard to locks and keys.
- Investigations with regard to the loss of keys reported or discovered.
- Compiling inventories with regard to locks and keys.
- Regular inspections with regard to keys and locks.
- Managing of the master and control keys.

- Ensure compliance with regard to regulations about locks and keys within the institution and its premises.

- Conducting maintenance and operation of the institution's keys depository (where keys to certain areas are issued and returned to the security office).

- Conduct periodic inventory inspections during which individuals are requested to verify possession of the keys for which the record indicates they are responsible.

- Training with regard to the setting of safe combinations.

- After hours visits to various security control points to determine if duplicate keys are managed correctly.

- Record keeping of statistics including the following:
  - Number of duplicate keys cut on a monthly basis.
  - How frequently combinations are reset or changed.
  - Number of padlocks cut (by means of a bolt cutter) on a monthly basis and an explanation of the reasons why the padlocks were cut.
  - Number of duplicate keys issued monthly and reasons why.
  - Number of use of the same key combinations.

(e) Any loss of keys must be reported immediately, in writing, to the key custodian after which the Security Manager will conduct an internal investigation and deal with the matter in terms of the security policy.

(f) Duplicate keys kept for emergency use must be sealed and stored in prescribed cabinets. Only the key custodian, Director: Technical and Security Manager can give permission to break a seal. At least one duplicate key must be kept in the key control room per directorate.

(g) In case a duplicate key is needed, a written motivation, countersigned by the Security Manager should be forwarded to the key custodian. This also applies when an employee leaves his/her keys at home.

(h) The duplicate keys of registries and other sensitive areas must be stored in a sealed envelope (with its details on the outside) by the custodian. A written record of the duplicate keys must be maintained.

(i) The key control officers/key custodian shall ascertain that duplicate keys are available and safeguard.

(j) Office keys must be returned to the key control officers/key custodian by employee who resign or are transferred, or for any reasons terminate their services with the Municipality. Where the circumstances are beyond control, for instance, due to death, their Directors must ensure they collect and submit the keys as in the case of access tags.

4.1.1.6 Cameras

No cameras that are carried by visitors are allowed into the buildings occupied by the Fezile Dabi District Municipality.

Cameras belonging to employees of the Municipality shall be dealt with in accordance of paragraph 4.1.1.1(f) of this policy.

Journalists with cameras visiting the buildings of the Municipality on official duty will be allowed to specified area after positive identification and confirmation of invitation by host.

4.1.1.7 Fire Arms

(a) All firearms belonging to employees and visitors must be declared to the security desks at the entry points. Firearm registers must be completed and signed by both owners and the Security Officers.

(b) The owner of a firearm will lock the firearm in the gun safes provided at the entry points before entering the premises.

(c) As the gun safes have two keys, the owner will be requested to keep one key and a Security Officer the other. The safe cannot be opened without both keys.

(d) In terms of Section 3 of the control of access to Public Premises and Vehicle Act (Act 53 of 1985), the members of the South African Police Service, National Intelligence Agency, South African National Defence Force and National Prosecution Authority (Scorpions) are exempted from both access and exit control if they are in the buildings to execute their official tasks.

(e) Separate arrangements must be in place to ensure that security officials, employees and visitors to the Municipality adhere to the Firearms Control Act, Act 60 of 2000.

(f) No firearms are allowed into the buildings in terms of the Firearms Act, (Act 60 of 2000). All buildings of the Municipality shall be declared gun free zones.

4.1.1.8 Office/Work Stations Security

(a) With regard to privileged information, the Fezile Dabi District Municipality has adopted a "clean desk policy". In a nutshell, this policy means that all valuable items (private or government owned) and sensitive/classified information must not be left unattended on desks, but must always be locked away if not in use.

(b) Employees are responsible for inspecting their own workstation/area/office for signs of intrusion at the beginning of each working day. If the employee detects any sign of intrusion, he/she must notify the immediate Senior Manager and thereafter, report the matter to the Security Manager.

(c) Cleaning of offices shall only be done during official working hours, supervised by the employee in the workstations/areas/offices. Work area/offices containing sensitive apparatus or documents that cannot be hidden/ locked away, should be cleaned by the employee in charge of the work station.

(d) Those who have offices must keep them locked at all times when they leave, even for a short period of time.

(e) Offices, cabinets, desk drawers, safes and/ or strong room keys must not be left hanging on doors, cabinets, desk drawers, safes and/ or strong rooms, or hidden in pot plants, behind fire equipment etc. but must be kept in the possession of the employee at all times.

(f) At the end of the day, before departure, the last employee to leave the workstation/ office should ascertain that:

(i) Lights and electrical appliances are switched off;
(ii) Blinds and curtains are drawn; and
(iii) Doors/ windows, safes and cabinets are closed/ locked.

(g) Human Resources Management shall advise all employees during induction that Fezile Dabi District Municipality is not responsible for loss or damage in respect of personnel (privately owned) property, as per Human Resources Policy.

4.1.1.9 Chamber

The Municipal chamber is the most significant and respectable place in the Municipality. The place needs to be treated as one of the houses of parliament.

- The chamber shall be locked at all the times, it will **only** be opened for the full council`s sittings.

- The Security Manager is the responsible person to control entrance to the chamber during meetings.

- Cleaning, maintenance and construction should be communicated to the Security Manager and time should play a pivotal role in this regard.

4.1.1.10 Buildings Patrol and Inspection

Security Manager shall ensure that all buildings accommodating the Fezile Dabi District Municipality are patrolled during office hours and in accordance with patrol plan drawn for Security Officers. A "Planned Inspection" shall be conducted once per month to determine the level of compliance. The Security Manager shall be responsible for conducting inspection. An assessment report with recommendations shall be submitted to the Senior Management at least seven days after inspection.

4.1.1.11 Emergency Management Plan

A contingency Plan is developed separately from this Policy. The plan is geared for saving lives, safeguarding property and information as well as ensuring that activities of Fezile Dabi District Municipality and the Office of the Executive Mayor and Speaker can continue with as little disruption as possible. The Disaster Department shall be the custodian of such policy and contingency officer must be appointed in writing for the Municipality by the Director: Health and Safety.

4.1.1.12 Sharing Accommodation

If Fezile Dabi District Municipality is sharing accommodation with other department/ private companies/ institutions the Municipality must establish a security forum with the other departments/ private companies/ institutions to implement security measures.

SECTION FIVE

5 REPORTING AND INVESTIGATION PROCEDURES FOR BREACHES OF SECURITY

(a) The objective is to prevent or reduce losses/ damages of money, property and the leakage of information of the Municipality.

(b) Burglary, theft and damage of state property in progress must be reported immediately to Security Manager.

(c) Thus, any employee who is aware or becomes aware of any deficiencies, losses or damage, whether caused by his/her improper application of security measures or not, must immediately, in writing, inform the Director: Financial Services. The following facts must be included in the report submitted to the Director: Financial Services;

(i) Serial number and description of assets and supplies. Full details pertaining to the circumstances that lead to the loss or damage; and

(ii) Name of eyewitnesses.

(d) An employee who is aware or becomes aware of any person who commits security breaches by not adhering to security measures shall immediately inform the Manager: Security Services. The Security Manager shall conduct an investigation to determine the circumstances that led to the security breaches and advise the person accordingly. Should such a person still not observe the security measures even after receiving advice, the incident will be referred to the immediate supervisor (i.e. Head of Department/ Chief Financial Officer/ Manager) of that person to take corrective measures. If the problem persists, all channels will be exhausted until the matter is referred to their supervisor (i.e. Head of Department/ Chief Financial Officer/ Manager) to institute disciplinary action in terms of Human Resource prescripts.

(e) In cases where a person who is aware of an irregularity suspects that his/ her identity may become known, or where the Security Manager is involved: he/ she shall report the irregularity/ security breaches to the Municipal Manager. (Protected Disclosure Act, Act 26 of 2000)

(f) The Security Manager and relevant Director where applicable shall immediately launch a preliminary investigation.

The purpose of the investigation shall be to:

(i) gather facts that can shed light on the irregularity/ security breaches;

(ii) report to management;

(iii) ascertain possible weakness (vulnerabilities and security measures) make recommendations; and

(iv) refer the matter to either the NIA, SAPS, Loss Control and/ or Labour Relations for further investigations.

(g) **Reporting of Losses, Damaged of Stolen Property**:

All incidents of loss, damage or stolen property of Fezile Dabi District Municipality must be reported by the employee concerned to Director: Financial Services.

All losses of state owned property such as safe keys, office keys, access tags, etc. must be reported to the immediate Director and thereafter to the Security Manager. The Director must ensure lost items mentioned above must be reported to SAPS. Before any claim can be made, a case number with a police statement on the cause of the loss must be submitted.

A written statement or, where applicable, a reporting form, must be completed as soon as possible and be handed in to the Security Manager.

The Security Manager shall conduct an internal investigation and/ or simultaneously, or at al later stage, refer the matter to the South African Police Service or to the National Intelligence Agency for further investigation.

Thereafter an investigation report comprising findings and recommend-dations will be submitted to Senior Management.

Note: Security measures/ procedures are not interested and should not be relaxed to cover up maladministration, corruption, criminal actions, etc, or to protect individuals/ officials involved in such cases.

SECTION SIX

6.1 COMMUNICATING THE POLICY

The Security Manager as the custodian will be responsible for communicating the policy and the following means of communications will be used:

- Induction of newly appointed employees, Internet, Information sessions, Road shows (district office), Booklets, Pamphlets and Billboards

6.2 REVIEW AND UPDATE PROCESS

The Security Manager will be responsible for the review and update process of the Security Policy assisted by the Security Committee.

The policy will be reviewed bi annually and whenever the need arises.

6.3 IMPLEMENTING THE POLICY

The Security Manager with the assistance of the Directors of all Departments in the Municipality are responsible to implement the Security Policy.

6.4 MONOTORING COMPLIANCE

The monitoring compliance of the Security Policy will be accomplished by:

6.1.1 Annual audits,
6.1.2 Site inspections,
6.1.3 Spot checks, and
6.1.4 After hour inspections.

SIGNATURE: _____ **DATE:** _____
S.M MOLALA
MUNICIPAL MANAGER

SIGNATURE: _____ **DATE:** _____
EXECUTIVE MAYOR
J.E.R.T. RAMOKHOASE

Annexure: B

NOTICE OF VISITS TO AREAS OUTSIDE THE BOUNDARIES OF RSA

1. Surname

2. Full Christian Names

3. Identity Number

4. Passport Number

5. Directorate: _____

6. Division: _____

7. Grade of Clearance: _____ Expiry Date: _____

8. Purpose of Visit:

Official	
Private	
Both	
Study	

9. Duration of Visit: From

D	M	Y

To

D	M	Y

10. Countries to be visited:

Country	Date of arrival D	Date of arrival M	Date of arrival Y	Date of departure D	Date of departure M	Date of departure Y

Where road transport is used, the border where applicable, must be mentioned.

11. Airline: Flight Number on Departure: _____

Flight Number on Arrival: _____

SIGNATURE DATE

This form must be completed by every official who has a security clearance. Should there be a deviation in the above schedule, an additional form must be complete on arrival in the RSA.

ANNEXURE: C

REMOVAL REGISTER CLASSIFIED DOCUMENTS

Date:..... **Received From** **Removed from:**..... **By** **(Members Name):**.....

Division:..... **Address where** **Documents will be kept:**.....

NO	REFERENCE	DATE	SUBJECT/DESCRIPTION	COPY VOL No	CLASSIFICATION		
					TS	S	C

1. Fill out in duplicate. One copy is to remain with the issuing institution.
2. Clearly indicate the classification/ status of the document in the appropriate column by means of an X e.g. Secret etc.
3. Remaining/ unused spaces must be indicated as such by drawing a diagonal line through it.
4. This form does not replace any mailing lists
5. Procedure in the event of documents being removed after hours.

5.1 All removed documents must be returned on the first following day

5.2 The controlling officer acknowledge/ indicates return of the removed documents by making a tick In the column marked NO (on the copy that remained in the register), and subsequently completes the adjacent Certificate

Documents indicated by a tick was returned

.....
SIGNATURE OF CONTROLLING OFFICIAL

Permission is granted for The removal of documents Removal is witnessed.

Signature of member receiving/ removing Documents

.....
Signature of Controlling Official/ Witness

.....

ANNEXURE: D

REMOVAL CERTIFICATE SECURITY SERVICES

Equipment removed from: _____ Destined Building: _____

Office No. Removed from: _____ Office Tel. Number: _____

Contact Person: _____ Contact Tel: _____

Building: _____

Security Services Component

Removal Permit

This is to grant permission for the under mentioned official/ visitor to remove the equipment/ material as indicated below. The security exit point is Fezile Dabi District Municipality Building: Name of Building where the equipment/ material is removed:

_____

Name of Official/ Visitor: _____ Persal Number: _____

I.D. Number: _____ Vehicle reg. No: _____

Description of Equipment/ Material. (Computer screen; overhead projector; photocopy paper)	Model (E.G Brother H.L-760 6 PPM/1200 dpi Quality)	Serial Number

Removal Authorised by: (Full names & Surname): _____
(Manager)

_____ _____ _____

Rank Date & Office Stamp Time

Equipment checked by Security Official: _____ at security point: _____

Date: _____ Time: _____

This form must be left at the security checkpoint and is only accepted by means of positive identification.