Annexure “A”

SECURITY POLICY AND STANDARD OPERATING PROCEDURES

SEDIBENG DISTRICT MUNICIPALITY
SITUATED AT:
CIVIC CENTRE BUILDING
Cnr.LESLIE & BEACONSFIELD STREETS

TABLE OF CONTENTS

1. SECURITY POLICY INTRODUCTION,DEFINITION AND PRINCIPLES

1.1 INTRODUCTION

A security policy is the essential basis on which an effective and comprehensive security program can be developed. The importance of this critical component of the overall security system, however, is often overlooked. A security policy is the primary way in which management's expectations for security are translated into specific and measurable goals and objectives. It is crucial to take a top down approach based on a well stated policy in order to develop an effective security system.

On the contrary, if there isn't a security policy defining and communicating those decisions, then they will made by the individuals designing, installing and maintaining security systems. This will result in a disparate and less than optimal security system being implemented.

1.2 DEFINITION

A security policy is a formal statement of the rules through which people are given access to an institution's premises, assets, and technology and information assets. The security policy should define what business and security objectives management desires, but not how these solutions are engineered and implemented.

A security policy should be economically feasible, understandable, realistic, consistent, and procedurally tolerable and also provide reasonable protection relative to the stated goals and objectives of management. Security policy should define the overall security and risk control objectives that Sedibeng District Municipality endorses. The characteristics of a good security policy are:

- It must be **implementable** through specific procedures and directives or other appropriate methods.
- It must be **enforceable** with security tools, where appropriate and with sanctions, where actual prevention is not technically feasible.
- It must clearly define the areas of **responsibility** for the different aspects of security (security personnel, staff and management) ; and
- It must be **documented, distributed** and **communicated**.

1.3 PRINCIPLES

T he security principles are an important step in security policy development as they dictate the specific type and nature of security matters most applicable to the environment of Sedibeng District Municipality.

The principles here are based upon the following goals:

- Creating a safe and secure working environment for the employees of the institution;
- Creating a safe and secure environment for members of the public visiting the institution ;
- Protecting the property of the institution;
- Protecting the proprietary information of the institution.

2. STATEMENT OF PURPOSE

Sedibeng District Municipality depends on its personnel, information and assets to deliver services that ensure safety and security of its stakeholders. It must therefore manage these resources with due diligence and take appropriate measures to protect them.

Threats that can cause harm to Sedibeng District Municipality, in South Africa and abroad, include acts of terror and sabotage, espionage, unauthorized access to buildings and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disasters, technical failures and accidental damage. The threat of cyber attack and malicious activity through the Internet is prevalent and can cause severe harm to electronic services and critical infrastructure. Threats to the national interest, such as transnational criminal activity, foreign intelligence activities and terrorism, continue to evolve as the results of changes in the international environment.

The Security Policy of Sedibeng District Municipality prescribes the application of security measures to reduce the risk of harm that can be caused to the institution if the above threats should materialize. It has been designed to protect political leaders, employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of services. Since Sedibeng District Municipality relies extensively on information and communication technology (ICT) to provide its services, this policy emphasizes the need for acceptable use of ICT equipment as well as ICT protection measures to be complied with by employees.

The main objective of this policy therefore is to support the interests of the community we serve and Sedibeng District Municipality business objectives by protecting employees, information and assets and assuring the continued delivery of services throughout the Sedibeng jurisdiction area and to South African citizens.

This policy complements other policies of Sedibeng District Municipality (e.g. sexual harassment, occupational health and safety, information management, asset control, real property, financial resources, supply chain management policy and contract management policy.)

3. SCOPE

3.1 This policy applies to the following (individuals and entities) resources:

- Executive Mayor, the Speaker, Mayoral Committee Members and Councilors
- The Municipal Manager, and all section 57 Managers
- All employees of Sedibeng District Municipality
- All contractors, consultants and service providers delivering a service to the Municipality, including their employees who may interact with this institution.
- Temporary employees of the Municipality
- All information assets of the Municipality
- All intellectual property of the Municipality
- All fixed property that is owned or leased by the Municipality
- All moveable property that is owned or leased by the Municipality

3.2 The policy further covers the following seven elements of the security program of the Municipality

- Security Organization
- Security Administration
- Information Security
- Physical Security
- Personnel Security
- Information and Communication Technology (ICT) Security
- Business Continuity Planning

4. LEGISLATIVE AND REGULATORY REQUIREMENTS

4.1 This policy is informed by and complies with applicable National legislation, National security policies and national security standards. A list of all applicable regulatory documents in this regard are as follows:

- Constitution Act of South Africa , 1996 (Act 108 of 1996)
- Control of Access to Public premises and Vehicles Act, 1985 (Act 53 of 1985)
- Criminal Procedure Act, 1977 (Act 51 of 1977)
- Extension of Security of Tenure Act, 1997 (Act 62 of 1997)
- Fire-arms Control Act, 2000 (Act 60 of 2000)
- Hazardous Substances Act, 1973 (Act 15 of 1973)
- Intimidation Act, 1982 (Act 72 of 1982)
- National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
- National Archives and Record Service of South Africa Act, 1996 (Act 43 of 1996) (Previous short title “National Archives of South Africa” substituted by s. 19 of Act 36 of 2001)
- National Strategic Intelligence Act, 1994 (Act 39 of 1994)
- Occupational Health and Safety Act, 1993 (Act 85 of 1993)
- Private Security Industry Regulation Act, 2001 (Act 56 of 2001)
- Promotion of Access to Information Act, 2000 (Act 2 of 2000)
- Protected Disclosures Act, 2000 (Act 26 of 2000)
- Protection of Information Act, 1982 (Act 84 of 1982)
- Public Service Act Proclamation 103 of 1994
- Public Service Regulations of 2001, which replaced the 1999 Regulations
- Security Officers Act, 1987 (Act 92 of 1987)
- Trespass Act, 1969 (Act 6 of 1969)
- MISS Policy , 1996

5. POLICY STATEMENT

5.1 General

This policy seeks to:

- Protect the Executive Mayor, Speaker, Mayoral Committee Members, Councilors, Accounting Officer, all employees and visitors to Sedibeng District Municipality against identified threats according to baseline security requirements and continuous risk management.
- To secure the information and assets of Sedibeng District Municipality against identified threats according to baseline security requirements and continuous risk management.
- To ensure continued delivery of services of Sedibeng District Municipality through baseline security requirements, including business continuity planning and continuous risk management.

5.2 Compliance Requirements

All individuals mentioned in paragraph 3.1 above must comply with baseline security requirements of this policy and it's associated Security Directives as contained in the Security Plan of Sedibeng District Municipality. These requirements shall be based on integrated security Threat and Risk Assessments (TRA's) to the interest of the Municipality and employees, information and assets of Sedibeng District Municipality. The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.

Security threat and risk assessments involve

- Establishing the scope of the assessment and identifying the information, employees and assets to be protected.
- Determining the threat to information, Politicians, employees and assets of the institution and assessing the probability and impact of threat occurrence.
- Assessing the risk based on the adequacy of existing security measures and vulnerabilities.
- Implementing any supplementary security measures that will reduce the risk to an acceptable level.

5.3 Staff accountability and acceptable use of assets

5.3.1 The Municipal Manager shall ensure that information and assets of the institution are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of Sedibeng District Municipality.

5.3.2 All employees of Sedibeng District Municipality shall be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse assets of the institution shall be held accountable therefore and disciplinary action shall be taken against any such employee.

5.4 Specific baseline requirements **5.4.1 Security administration** 5.4.1.1 The functions referred to in paragraph 5.3.1 above include: • General security administration (departmental directives and procedures, training, and security awareness, security risk management, security audits, sharing of information and assets) • Setting of access limitations • Administration of security screening • Implementation of physical security • Ensuring the protection of employees • Ensuring the protection of information • Ensuring ICT security • Ensuring security in emergency and increased threat situations • Facilitating business continuity planning • Ensuring security in contracting • Facilitating security breach reporting and investigations • Implementation Strategy. **5.5 Security incident/breaches reporting process** 5.5.1 Whenever employees of the institution become aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidental or intentional), they must report this to the Security Manager of the institution by utilizing the formal reporting procedure prescribed by the Security Breach Directive of the institution. 5.5.2 The Security Manager shall report to the appropriate authority (as indicated in the Security Breach Directive) of the institution all cases or suspected cases of security breaches for investigation. 5.5.3 The Security Manager of the institution shall ensure that all employees are informed about the procedure for reporting security breaches. **5.6 Security incident/breaches response process** 5.6.1 The Security Manager shall develop and implement security breach response mechanisms for the institution in order to address all security breaches/alleged security breaches which are reported. 5.6.2 The Security Manager shall ensure that the Accounting Officer and ED: Corporate Services are informed and advised as soon as possible. 5.6.3 It shall be the responsibility of the National Intelligence structures (e.g. NIA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the institution. 5.6.4 Access privileges to classified information, assets and/or to premises may be suspended by the Municipal Manager until administrative, disciplinary and/or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches.	See Security Directive on Reporting of Security Breaches.

5.6.5 The end result of these investigations, disciplinary actions or criminal prosecutions may be taken into consideration by the Municipal Manager in determining whether to restore or limit the security access privileges of an individual or whether to revoke or alter the security clearance of the individual.	
5.7 Information security	
5.7.1 Categorization of information and information classification system	
5.7.1.1 The Security Manager must ensure that a comprehensive information classification system is developed and implemented in the institution. All sensitive information produced or processed in the institution must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.	See Security Directive on Information Security / Categorization of information and information classification.
5.7.1.2 All sensitive information must be categorized into one of the following categories. • State Secret • Trade Secret: and • Personal Information • Shared information and subsequently classified according to its level of sensitivity by using one of the recognized levels of classification: • Confidential • Secret: and • Top Secret	
5.7.1.3 Employees of the institution who generates sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labeling of classified documents.	
5.7.1.4 The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times.	
5.7.1.5 Access to classified information will be determined by the following principles: • Intrinsic secrecy approach • Need-to-know • Level of security clearance.	

5.8 Physical Security

5.8.1 Physical security involves the physical layout and design of facilities of Sedibeng District Municipality and the use of physical security measures to delay and prevent unauthorized access to assets of the institution. It includes measures to detect attempted or actual unauthorized access and the activation of an appropriate response. Physical security also includes the provision of measures to protect employees from bodily harm.

See Security Directive on Physical Security Procedures.

5.8.2 Physical security measures must be developed, implemented and maintained in order to ensure that the entire Municipality, its personnel, property and information are secured. These security measures shall be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Manager.

5.8.3 Sedibeng District Municipality shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities. The Municipality shall:

- Select, design and modify facilities in order to facilitate the effective control of access thereto.
- Demarcate restricted areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto.
- Include the necessary security specifications in planning, request for proposals and tender documentation.
- Incorporate related costs in funding requirements for the implementation of the above.

5.8.4 Sedibeng District Municipality will also ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms.

5.9 Personnel Security

5.9.1 Security Screening

5.9.1.1 All newly appointed employees, contractors and consultants attached to Sedibeng District Municipality, who requires access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security screening investigation conducted by the National Intelligence Agency (NIA) in order to be granted a security clearance at the appropriate level.

See Security Directive on Vetting/Personnel Suitability Checks.

5.9.1.2 The level of security clearance given to a person will be determined by the contents of or access to classified information entailed by the post already occupied or to be occupied in accordance with their respective responsibilities and accountability.

5.9.1.3 A security clearance provides access to classified information subject to the need-to-know principle.

5.9.1.4 A declaration of secrecy shall be signed by every individual issued with a security clearance to complement the entire security screening process. This will remain valid even after the individual has terminated his/her services with the Municipality.

5.9.1.5 A security clearance will be valid for a period of ten years in respect of Confidential level and five years for Secret and Top Secret. This does not preclude re-screening on a more frequent basis as determined by the Municipal Manager, based on information which impact negatively on an individual's security competency.

5.9.1.6 Security clearances in respect of all individuals who have terminated their services with the Municipality shall be immediately withdrawn.

5.10 Polygraph Screening

5.10.1 A polygraph examination shall be utilized to provide support for the security screening process. All employees subjected to a Top Secret clearance will also be subjected to a polygraph examination. The polygraph shall only be used to determine reliability of the information gathered during the security screening investigation and does not imply any suspicion or risk on the part of the person being examined.

5.10.2 In the event of any negative information being obtained with regard to the person being examined during the security screening investigation (all levels), such person shall be given an opportunity to prove his/her honesty and/or innocence by making use of a polygraph examination. Refusal by the applicant to undergo the examination does not necessarily signify that a security clearance will not be granted.

5.11 Transferability of security clearances

5.11.1 A security clearance issued in respect of an official from other Government institutions shall not be automatically transferable to Sedibeng District Municipality. The responsibility for deciding whether the official should be re-screened rests with the Municipal Manager.

5.12 Security Awareness and Training

5.12.1 A security awareness and training program must be developed by the Security Manager and implemented to effectively ensure that all personnel and service providers of the Municipality remain security conscious.

5.12.2 All employees shall be subjected to the security awareness and training programs and must certify that the contents of the program(s) have been understood and will be complied with. The program must cover training with regard to specific security responsibilities and sensitize employees and relevant contractors and consultants about the security policy and security measures of the Office of the Executive Mayor and the need to protect sensitive information against disclosure, loss or destruction.

5.12.3 Periodic security awareness presentations, briefings and workshops will be conducted as well as posters and pamphlets frequently distributed in order to enhance the training awareness program. Attendance of the above programs is compulsory for all employees identified and notified to attend the events.

5.12.4 Regular surveys and walkthrough inspections will be conducted by the Security Manager and members of the security component to monitor the effectiveness of the security awareness and training program.	
5.13 Information and Communication Technology (ICT) Security	
5.13.1 IT Security	
5.13.1.1 A security network shall be established for the Municipality in order to ensure that information systems are secured against rapidly evolving threats that have the potential to impact on their confidentiality, integrity availability, intended use and value.	See IT and ICT Policy to be compiled.
5.13.1.2 To prevent the compromise of IT systems, the Municipality shall implement baseline security controls and any additional controls identified through the security TRA. These controls, and the security roles and responsibilities of all personnel, shall be clearly defined, documented and communicated to all employees.	
5.13.1.3 To ensure policy compliance, the IT Director of the Municipality shall: • Certify that all IT systems are secure after procurement, accredit IT systems prior to operation and comply with minimum security standards and directives. • Conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis. • Periodically request assistance, review and audits from the National Intelligence Agency (NIA) in order to get an independent assessment.	
5.13.1.4 Server rooms and other related security zones where IT equipment are kept shall be secured with adequate security measures and strict access control shall be enforced and monitored.	
5.13.1.5 Access to the resources on the network of the institution shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of the institutions shall be restricted unless explicitly authorized.	
5.13.1.6 System hardware, operating and application software, the network and communication systems of the institution shall all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.	
5.13.1.7 All employees shall make use of IT systems of the institution in an acceptable manner and for business purposes only. All employees must comply with the IT Security Directives in this regard at all times.	
5.13.1.8 The selection of passwords, their use and management as a primary means of access to systems is to strictly adhere to best practice guidelines as reflected in the IT Security Directives; in particular, passwords shall not be shared with any other person for any reason.	
5.13.1.9 To ensure the ongoing availability of critical services, the institution shall develop IT continuity plans as part of the overall Business Continuity Planning (BCP) and recovery activities.	

5.14 Internet Access

5.14.1 The IT Director of the Municipality, having the overall responsibility for setting up Internet access for the institution, shall ensure that the network of the institution is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Human Resources management shall ensure that all personnel with Internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet.

5.14.2 The IT Director of the institution shall be responsible for controlling user access to the Internet, as well as ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security Breaches and incidents.

5.14.3 Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible computer viruses or other malicious code.

5.15 Use of Laptop Computers

5.15.1 Usage of laptop computers by employees of the Municipality is restricted to business purposes only, and users shall be aware of and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.

5.15.2 The information stored on a laptop computer of the institution shall be suitably protected at all times, in line with the protection measures prescribed in the IT Policy.

5.15.3 Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop computers at all times, inline with the protection measures prescribed in the IT policy.

5.16 Communication Security

5.16.1 The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of the Office of Executive Mayor, Speaker, MMC's, Municipal Manger and Sec 57 Managers in all its forms and at all times.

5.16.2 All sensitive electronic communication by employees, contractors or employees of the institution must be encrypted in accordance with the South African Communication Security Agency (SACSA) standards, COMSEC standards and the Communication Security Directive of the institution. Encryption devices shall only be purchased from SACSA or COMSEC and will not be purchased from commercial suppliers.

5.16.3 Access to communication security equipment of the Municipality and the handling of information transmitted and/or received by such equipment, shall be restricted to authorized personnel only (personnel with a Top Secret Clearance who successfully completed the SACSA Course).

5.17	**Technical Surveillance Counter Measures (TSCM)**	
5.17.1	All offices, meeting, conference and boardroom venues of the Municipality where sensitive and classified matters are discussed on a regular basis shall be identified and shall be subjected to proper and effective physical security and access control measures. Periodic electronic Technical Surveillance Counter Measures (sweeping) will be conducted by the National Intelligence Agency (NIA) to ensure that theses areas are kept sterile and secure.	See Security Directive on TSCM.
5.17.2	The Security Manager of the Municipality shall ensure that areas that are utilized for discussion of a sensitive nature as well as offices or rooms that house electronic communications equipment, are physically secured in accordance with the standards laid down by National Intelligence Agency (NIA) in order to support the sterility of the environment after a TSCM examination, before any request for a TSCM is submitted.	
5.17.3	No unauthorized electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of the institution is discussed. Authorization must be obtained from the Security Manager.	
5.18	**Business Continuity Planning (BCP)**	
5.18.1	Both the Security Manager and IT Director must establish a Business Continuity Plan (BCP) to provide for the continued availability of critical services, information and assets if a threat materializes and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of the employees, contractors, consultants and visitors.	See Business Continuity Planning to be compiled.
5.18.2	The BCP shall be periodically tested to ensure that the management and employees of the Municipality understand how it is to be executed.	
5.18.3	All employees of the institution shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.	
5.18.4	The Business Continuity Plan shall be kept up to date and re-tested periodically by the Security Manager and IT Director.	
6.	**SPECIFIC RESPONSIBILITIES**	
6.1	**Head of Institution**	
6.1.1	The Municipal Manger bears the overall responsibility for implementing and enforcing the security program of the institution, Towards the execution of this responsibility, the Executive Director:Coporate Services shall: • Establish the post of the Security Manager and appoint a well trained and competent security official in the post. • Establish a security committee for the institution and to ensure the participation of all senior management, members of all the core business functions of the institution in the activities of the committee • Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.	See Security Administration and organization Directives

6.2 Security Manager

6.2.1 The delegated security responsibilities lies with the Security Manager of the Municipality who will be responsible for the execution of the entire security function and program of the institution (coordination, planning, implementation, controlling, etc). Towards execution of his/her responsibilities, the Security Manager shall, amongst others:

- Chair the security committee of the Municipality
- Draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of the institution in conjunction with the security committee.
- Review the Security Policy and Security Plan at regular intervals.
- Conduct a security TRA of the institution with the assistance of the security committee
- Advise management on the security implication of management decisions
- Implement a security awareness program
- Conduct internal compliance audits and inspection at the Municipality at regular intervals.
- Establish a good working relationship with both the SAPS and the NIA and liaise with these institutions on a regular basis.
- As mentioned in paragraph 6.2.1 Security Manager should have delegated signing powers as per Municipal Manager's and Executive Director: Corporate Service's discretion.

6.3 Security Committee

6.3.1 The Security Committee referred to in paragraph 5.1.1 above shall consist of senior managers of the Municipality representing all the main business units of the Municipality.

6.3.2 Participation in the activities of the Security Committee by the appointed representatives of business units in the Municipality shall be compulsory.

6.3.3 The Security Committee of the Municipality shall be responsible for, amongst others:

6.3.4 Assisting the Security Manager in the execution of all security related responsibilities of the Municipality, including completing tasks such as drafting/reviewing of the Security Policy and Plan, conducting of a security TRA, conducting of security audits, drafting of a BCP and assisting with security awareness and training.

7. DIRECTORS/LINE MANAGERS

7.1 All managers on the Municipality shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of the Municipality.

7.2 All managers must ensure that appropriate measures are implemented and steps are taken immediately to rectify any non compliance issues that may come to their attention. This includes the taking of disciplinary action against employees if warranted.

8. EMPLOYEES, CONTRACTORS, CONSULTANTS AND OTHER SERVICE PROVIDERS

8.1 Every employee, Contractor, Consultant and other Service Providers of Sedibeng District Municipality shall know what their security responsibilities are, accept it as part of their normal job function, and not only cooperate but contribute to improving and maintaining security at the institution at all times.

9. STAKEHOLDERS

9.1 This policy is applicable to all members of the management, employees, consultants, contractors and any other service provider of Sedibeng District Municipality. It is further applicable to all visitors and members of the public visiting premises of or may officially interact with the institution.

10. ENFORCEMENT

10.1 The Municipal Manager, Executive Director: Corporate Services and the appointed Security Manager are accountable for the enforcement of this policy.

10.2 All employees of the institution are required to fully comply with this policy and it's associated Security Directives as contained in the Security Plan. Non-compliance with any prescript shall be addressed in term of the Disciplinary Code/Regulations of the Municipality.

10.3 Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of the Municipality shall be included in the contracts with such individual/institutions/companies. The consequences of any transgression/deviation or n on-compliance shall be clearly stipulated in the said contract and shall be strictly enforced. Such consequences may include the payment of prescribed penalties or termination of the contract, depending on the nature of any non-compliance.

11. EXCEPTIONS

11.1 Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:

- When security must be breached in order to save or protect the lives of people.
- During unavoidable emergency circumstances e.g. natural disasters.
- On written permission of the Security Manager (reasons for allowing non-compliance to one or more aspects of the policy and directives shall be clearly stated in such permission: no blanket non-compliance shall be allowed under any circumstances).

12. OTHER CONSIDERATIONS

12.1 The following shall be taken into consideration when implementing this policy:

12.2 Occupational Health and Safety issues of Sedibeng District Municipality.

12.3 Disaster Management of the Sedibeng District Municipality.

12.4 Disabled people shall not be inconvenienced by physical security measures and must be catered for in such a manner they have access without compromising security or the integrity of this policy.

12.5 Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).

13. COMMUNICATION POLICY

13.1 The Security Manager of Sedibeng District Municipality shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees, consultants, contractors, service providers, clients, visitors, members of the public that may officially interact with the institution). The Security Manager will further ensure that all security policy and directive prescription are enforced and complied with.

13.2 The Security Manager must ensure that a comprehensive security awareness program is developed and implemented within the Municipality to facilitate the above said communication. Communication of this policy by means of this program shall be conducted as follows:

- Awareness workshops and briefings to be attended by all employees.
- Distribution of memos and circulars to all employees.
- Access to the policy and applicable directives on the intranet of the institution.

14. PARKING POLICY

14.1 Purpose

The purpose of the policy is to establish clearly the principles by which parking administration and allocations are made at all Sedibeng District Municipality Offices and Buildings. It is also intended to define the regulations for parking in municipal allocated sites.

14.2 Scope

This policy applies to all transactions in which the Municipality provides parking spaces for Councillors, Employees, Monthly Rental Customers and Visitors.

14.3 Responsibility

The overall responsibility for the administration and interpretation of this policy lies with Facilities Management Directorate.

15. POLICY

15.1 Basic Principles

a. Parking under the auspices of the Municipality will include all spaces on Municipal property.
b. Parking will not be subsidised by the Municipality, but rates must be established

based on a cost effective approach to the administration of parking and must be competitive.

c. Priority will be given to applicants with physical disability.

15.2 Apportionment of costs and responsibilities

a. The Facilities Management Directorate will oversee the parking policy and annually set a fee, including fines for use of the parking spaces.
b. The annual fee will include all direct costs of operating and maintaining municipal owned properties used for parking.
c. The Department: Facilities Management Directorate will:

- Assign and transfer Management of parking spaces and maintain a waiting list for additional requests security service provider.
- Transfer the responsibility of maintains a list of parking spaces and the persons assigned to these spaces.
- Transfer the responsibility of managing, maintain and supervision of all SDM Parking facility for the specified contracted period.
- Recommend the monthly fixed fee per annum for use of the parking spaces to Finance Department. Costs will be determined so that all municipal Full Time Councillors, Senior Management and Employees are charged a standard fee equal to everyone.
- Recommend the annual fixed fee per annum for use of the public oriented parking facility to Finance Department. Costs will be determined by daily business operations of that specific parking that all rental customer/clients are charged a standard fee.
- Arrange for the collection of fees from the individuals and ensure prompt payment.
- Maintain and update procedures.

d. The security service provider will be responsible for loss of or damage to vehicles or contents.

15.3 Allocation of parking spaces

a. All employees and those with physical disability may apply for parking.
b. Parking spaces will be allocated, as space is available, to municipal employees and to those with physical disability.
c. Some spaces will be reserved for Full Time Councillors and Senior Management.

d. Parking spaces will be allocated on the bases of the following criteria:

- Physical disability.
- Seniority.
- Deliveries including IT.
- Other factors that are considered to be of importance.

e. The Municipality offers daytime parking only.
f. A municipality vehicle is automatically qualified for the allocation of a reserved parking space on application by the relevant departmental manager

15.4 Penalties

a. Abuse of any of the parking regulations outlined above may result in a loss of parking privileges, payment of a fine and or prompt removal of the vehicle by the designated towing company at the cost of the employee.

16. PROCEDURES

16.1 Applications for parking spaces – employees

a. All employees who wish to have parking space shall complete and sign a parking application each year. Applications are available at Facilities Management Directorate to security service provider.
b. Upon allocation of a parking space, the signed application shall become the parking contract.
c. Normally, all parking spaces shall be allocated annually for the period of 01st July to 30th June. Except in the case of termination of employment, cancellations shall be accepted only if the space can be re-assigned from the waiting list. One month notice must be given for cancellation.

16.2 Special Parking Arrangements

a. Special parking arrangements may be arranged through Facilities Management Directorate.
b. Limited visitor parking may be available from time to time with arrangements through Facilities Management Directorate.

16.3 Use of parking permit – all employees

a. All approved applicants shall be issued out with a formal parking permit signed by Security Manager.
b. Parking permits are not transferable. However arrangements to lend a parking space to another employee during a temporary absence may be allowed on condition that it is reported to Security Manger.
c. An authorized parking permit must be displayed, totally unobstructed as per instructions, when parked in municipal designated parking.
d. Parkers must use only those spaces to which they have been assigned.
e. The must only be one vehicle per authorized Parker parked in municipal allocated space at any given time.
f. Any change in vehicle or licence number must be reported to Facilities Management (Security Manger) as quickly as possible.
g. Where more than one vehicle is registered, the parking permit is transferable from one vehicle to the other at the discretion of the holder of the parking permit
h. Except in the case of an emergency, maintenance and repairs to vehicles on Municipal property is not permitted. All waste materials must be promptly removed from Municipal property.

16.4 Management of Parking Committee members

1. Director: Facilities Management Directorate – Chairperson
2. Security Manager- Deputy Chairperson
3. Accountant Income –SDM Finance Department
4. Senior Security Officer
5. Directors:Secuirty Service Provider (Futuris Guarding Systems (PTY)LTD
6. Site Operations Manager (Futuris Guarding Systems (PTY) LTD.

17. EFFECTIVE DATE

This policy shall be applicable immediately after approval by Council and shall replace all parking arrangements entered into in the past. The policy shall be reviewed annually by Facilities Management Directorate.

18. REVIEW AND UPDATE PROCESS

18.1 The Security Manager, assisted by the Security Committee of the Municipality, must ensure that this policy and its associated Security Directives is reviewed and updated on an annual basis. Amendments shall be made to the policy and directives as the need arise.

19. IMPLEMENTATION

19.1 The Security Manager of the Municipality must manage the implementation process of this policy and its associated Security Directives (contained in the Security Plan) by means of an action plan (also to be included in the Security Plan of the Municipality).

19.2 Implementation of the policy and its associated Security Directives is the responsibility of each and every individual this policy is applicable to (see paragraph 3.1 above).

20. MONITORING

20.1 The Security Manager, with the assistance of the security component and the Security Committee of the Municipality must ensure compliance with this policy and it's associated Security Directives by means of conducting internal security audits and inspection on a frequent basis.

20.2 The findings of the said audits and inspections shall be reported to the Municipal Manager forthwith after completion.

21. DISCIPLINARY ACTIONS

21.1 Non-compliance with this policy and its associated Security Directives shall result in disciplinary action which may include but are not limited to :

- Re-training
- Verbal and written warnings
- Termination of contracts in the case of contractors or consultants delivering a service to the institution.
- Dismissal
- Suspension
- Loss of institution information and asset resources access privileges.

21.2 Any disciplinary action taken in terms of non-compliance with this policy and its associated directives will be in accordance with the disciplinary code/directives of the institution.

22. DEFINITION OF TERMS

22.1 Access Control

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

22.2 Classification

22.2.1 The process whereby all official matters exempted from undue disclosure is labelled Confidential, Secret or Top Secret.

22.3 Contingency Planning

23.3.1 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.

22.4 Computer Security

22.4.1 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.

22.4.2 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.

22.5 Communication Security

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

22.6 Declaration of Secrecy

2.6.1 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.

22.7 Delegation

22.7.1 Delegation is the transfer of authority, powers or functions from one person/department to another.

22.8 Document

22.8.1 In terms of the Protection of Information Act, 1982 (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.

22.9 Document Security

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

22.10 Employees

22.10.1 For the purpose of this policy the term employees includes:

Permanent staff;
Temporary staff; and
Contract staff.

22.11 Information Security

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

22.12 Personnel security

22.12.1 Personnel security is that condition created by the conscious provision and application of security measures in order to ensure that any person who gains access to 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.

22.13 Physical security

22.13.1That condition which is created by the conscious provision and application of physical security measures for the protection of persons, property and information.

22.14 Premises

22.14.1 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 Sedibeng District Municipality and to which a member of the public has a right of access.

- **SANDF**- South African National Defence Force
- **SAPS**- South African Police Service
- **SASS**- South African Secret Service
- **NIA**- National Intelligence Agency

22.15 Screening Institution

22.15.1 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.

22.16 Security

22.16.1 Security is the condition free of risk or danger, created by the conscious provision and application of security measures.

22.17 Security audit

22.17.1 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.

22.18 Security clearance

22.18.1 It is a process whereby an official is given access to official documents in line with the inherent requirements of the job, indicating the degree of security competence of such an official (s). An official document that indicates the degree of security competence of a person.

22.19. Visitors

22.19.1 Members of the public.

22.20 Contractors/Service Providers

22.20.1 Any individual or company rendering a service to Sedibeng District Municipality, whether caterers, contractors etc.

24. SUPPORTING DOCUMENTS

24.1 Security Plan containing the following:

- Security Component Organizational Structure
- Security Component SOP,s
- Specific Responsibilities of Key Role Players
- Security Directive: Reporting of Security Breaches
- Security Directive: Security Breaches Response Procedures
- Security Directive: Information Security: General Responsibilities
- Security Directive: Classification System
- Security Directive: Security Screening
- Security Directive: Physical Security
- Security Directive: Access Control
- Security Directive: ICT Security
- Security Directive: Secure Discussion Areas
- Security Directive: TRA
- Security Directive: Security Audits and Inspections
- ICT Security Policy
- BCP
- OHS Policy
- Disciplinary Code
- Supply Chain Management Policy
- Contract Management Policy

APPROVAL OF THE POLICY:

Document Name	**Security Policy and Procedures**	
Signature	_____ **MUNICIPAL MANAGER**	_____ **Date:**
Adopted by the Mayoral Committee	_____ **CHAIRPERSON**	_____ **Date:**
Approved by the Council	_____ **RESOLUTION**	_____ **Date:**

Effective date: _____

Next revision date: _____

SECURITY DIRECTIVE

TO: ALL EMPLOYEES	FROM: DIRECTOR:FACILITIES MANAGEMENT DIRECTORATE REF : SECURITY MANAGER
CC: MUNICIPAL MANAGER ALL EXECUTIVE DIRECTORS CHIEF FINANCIAL OFFICER ALL PMT,s OFFICES	DATE: 27 SEPTEMBER 2010

SECURITY DIRECTIVE 1: File Nr 8/2/2/81-2010

Re: REPORTING OF SECURITY BREACHES

The objective is to prevent, reduce losses/damages and misuse assets and leakage of information of Sedibeng District Municipality.

Reporting procedures

1. *Burglary, theft, damage and misuse of assets in progress must be reported immediately to the Security Manager.*

2. *Any employee who is aware or becomes aware of any deficiencies, losses, damages and misuse whether caused by his/her improper application of security measures or not must immediately, in writing inform the Security Manager. The following facts must be included in the report submitted to the Security Manager;*

   - *Serial number and description of assets*
   - *Full details pertaining to the circumstances that led to the loss, damage and misuse of assets*
   - *Name of eyewitnesses*

3. *An employee who is aware or becomes aware of any person who commits security breach by not adhering to the security measures shall immediately inform the Security Manager. The Security Manager shall conduct an investigation to determine the circumstances that led to the security breach and advice the person accordingly. Should that person still not observe the security measures even after*

receiving advice, the incident will be reported to the to the immediate Executive Director and Director to institute corrective measures in terms of Human Resources prescripts.

4. *In cases where a person is aware of the irregularity suspect that his/her identity may become known, or where the Security Manager is involved, he/she shall report the irregularity to the Municipal Manager and Protected Disclosure Act 26 of 2000 will be invoked.*

Reporting of loss, damage, stolen and misuse of assets

- *All incidents of loss, damage, stolen and misuse of assets of Sedibeng District Municipality must be reported by the employee concerned to the Chief Financial Officer and Security Manager.*

- *All losses of Sedibeng District Municipality assets such as safe keys, access tags etc, must be reported to the immediate Executive Director and thereafter to the Security Manager. The Security Manager must ensure lost items mentioned above are reported to the South African Police Service. Before any claim can be made, a case number with a police statement on the cause of the loss or damage 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 the later stage refer the matter to the South African Police Service or National Intelligence Agency.*

Thereafter an investigation report comprising of findings and recommendations will be submitted to the Executive Director: Corporate Services and the Municipal Manager.

Recommended / Not Recommended

....
ED: Corporate Services *Date*
Adv Mosotho Petlane

Approved / Not Approved

....
Municipal Manager *Date*
Mr Yunus Chamda

SECURITY DIRECTIVE

TO: ALL EMPLOYEES	FROM: DIRECTOR:FACILITIES MANAGEMENT DIRECTORATE REF: SECURITY MANAGER
CC: MUNICIPAL MANAGER ALL EXECUTIVE DIRECTORS CHIEF FINANCIAL OFFICER ALL PMT,s OFFICES	DATE: 27 SEPTEMBER 2010

SECURITY DIRECTIVE 2: File Nr 8/2/2/84-2010

Re: Information Security

The objective of the directive is to describe the classification of information (contained in documents, patents, plans, etc), is the assignment of the relevant contents of the information, by way of e.g. a mark or seal, to one of the acknowledged categories of secrecy which shall be implemented in SDM facility for protection against unauthorized access and damage to interference with information.

*The acknowledged categories of secrecy relating to **state (municipality) secrets**, **trade secrets** and **personal information** are as follows which must be adhered to at all the times.*

Categories of secrecy

5. *Top secret*

- *This category should be reserved for use in exceptional circumstances only i.e. instances where a document would be classified as such, would be if a document contains information:*

    I. *which forms the municipality secret and where the disclosure of the information would cause serious and irreparable harm to the security*

or interest of the municipality or may cause other states to sewer diplomatic relations with the Republic.

II. *which constitutes a trade secret the disclosure of which would have disastrous results with regard to the future existence of the municipality, cause financial loss to the municipality or may cause embarrassment to the municipality in its relations with its clients,public,outside contractors, competitors and suppliers .*

III. *which is personal information the disclosure of which would endanger the life of the individual or in the case of an employee, where the information is information that the municipality does not wish its employees in the personnel section should be aware of (such as information gathered during an investigation of the employee's personal life for the purposes of a security clearance).*

6. Implementation of the system of information classification

I. *It is the responsibility of the Municipal Manager to ensure that a document in the possession or under the control of SDM and which falls under one of the aforementioned categories of information is properly classified in accordance with the category of which it forms part.*
II. *All classified documents must be stored in accordance with instructions while not in use.*
III. *All incoming classified documents, including official, classified post marked "Personal" must be received and noted in a register by persons with the appropriate clearance.*
IV. *Officials who usually receive the incoming post of SDM (e.g. registration officers) must hand the unopened inner envelope of incoming classified correspondence to the appropriate official(s) who is/are authorised to open correspondence in a certain category.*
V. *All classified documents that are dispatched, made available or distributed, must be subjected to record keeping in order to ensure control thereof. This provision does not apply to documents that are classified as Restricted.*
VI. *Measures must be taken to ensure that classified documents are not physically taken from one institution during a contact visit, in this way evading prescriptions for the registration of incoming and outgoing post.*
VII. *When Secret and Top Secret documents are distributed, dispatched or made available, they must be accompanied by a receipt voucher signed by the addressee and escorted by security officers if a need arose (i.e. FACE VALUE DOCUMENTS),the receipt of which must again be controlled by sender. The receipt voucher is classified only if the subject/heading of the document itself is classified only if the subject/heading of the document*

itself is classified, in which the case the classification must agree with that of the document.

VIII. *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 7copies.*

7. Handling of classified information

As an approved custodian or user of classified information, an employee with a security clearance is personally responsible for the protection and control of the information entrusted to him/her. They must safeguard this information at all times to prevent loss or compromise and unauthorized disclosure, dissemination or duplication thereof.

Unauthorized disclosure of classified information or material is punishable under e.g. the Public Service Act, Protection of information Act.

The Security Manager must brief employees on the specific rules for handling classified information.SDM should adopt and implement the following standard procedures that apply to everyone:

I. *Classified information that is not secured in an approved security container or officer shall be constantly under the control of a person having the proper security clearance and following the need-to-know principle strictly.*
II. *And end-of-day security check should ensure that all classified information or material is properly secured before closing for the day.*
III. *If an employee should find classified information or material left unattended (e.g. in a boardroom, on an office desk or rest room), it is his /her responsibility to ensure that the information or material is properly protected. He /she should stay with the classified information or material and notify the security manager or component. If not possible the documents must be taken to a supervisor or another person with authorized access to that information, or, if necessary the material must be locked away in his/her own safe or cabinet overnight.*
IV. *Classified material should not be taken home. Employees must not work on classified information or material (e.g. Tender documents) at home without approval in writing from delegated person (e.g. Executive Director, Chief Financial Officer or Municipal Manager).*
V. *Classified information must not be disposed of in a waste basket. It must be placed in a designated container for an approved method of destruction such as shredding or burning.*
VI. *E-mail and the internet create many opportunities for inadvertent disclosure of classified information. Before sending an e-mail, posting to a bulletin board, publishing anything on the internet, or adding to an existing Web page, employees must be absolutely certain none of the information is*

classified or sensitive information. Employees must be familiar with the SDM IT policy for use of the internet. Classified and sensitive information MUST be encrypted before it can be sent via e-mail. It must also ONLY be faxed by means of an encrypted fax machine (only SACSA equipment/software may be used for this purpose).

VII. *Classified working papers such as notes and rough drafts should be dated when created, marked with the overall classification and with the annotation "Draft Only" and disposed of with other classified waste when no longer needed.*

VIII. *Computer diskettes, magnetic tape,CDs,DVDs, carbon paper and used typewriter ribbons may pose a problem when doing a security check, as visual examination does not readily reveal whether the items contain classified information. To reduce the possibility of error, SDM should treat all such items as classified even though they may not necessarily contain classified information.*

IX. *Secret and Top Secret information is subject to continuing accountability. Receipts or File Nr must be used to control the distribution and keeping of information classified to these levels. Each item of Secret and Top Secret material must be numbered in series and each copy also numbered. It must also include a distribution list.*

Recommended / Not Recommended

....
Executive Director: Corporate Services *Date*
Adv Mosotho Petlane

Approved / Not Approved

....
Municipal Manager *Date*
Mr Yunus Chamda

SECURITY DIRECTIVE

TO: ALL EMPLOYEES	FROM: DIRECTOR:FACILITIES MANAGEMENT DIRECTORATE REF: SECURITY MANAGER
CC: MUNICIPAL MANAGER ALL EXECUTIVE DIRECTORS CHIEF FINANCIAL OFFICER ALL PMT,s OFFICES	DATE: 27 SEPTEMBER 2010

SECURITY DIRECTIVE 3: File Nr 8/2/2/80-2010

Re: PHYSICAL SECURITY PROCEDURES

The objective of the directive is to describe minimum physical preventative, detection, corrective security measure which shall be implemented in Sedibeng District Municipality facility for protection against unauthorized access and damage to interference with information

The following security procedures are compulsory and must be adhered to at all the times.

Physical Security measures

8. ***Access control***.

- *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.*

- *No persons shall, without the permission of the Security Steward/Officer enter any of the buildings occupied by Sedibeng District Municipality.*

- *For the purpose of granting of permission the Security Officer may request that the person concerned;*

- *Furnish his/her name, address and any other relevant information required by the authorized Officer,*
- *Produce his/her identity to the satisfaction of the authorized Officer,*
- *Declare whether he/she has any dangerous object i.e. Firearm in his/her possession or custody,*
- *Declare the nature of the contents of any suitcase, attaché` 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 for examination by electronic or other apparatus in order to determine the presence of any dangerous object(s),*
- *Hand to an authorized Officer anything, that he/she has in his/her possession or custody for examination or custody until he/she leaves the premises*

9. Exit control and movements of assets

All vehicles (private or municipal owned) may be searched when leaving the building occupied by SDM. Equipments, parcels, documents etc shall be taken out of the building with official removal permit signed by authorized official.

(a) All identified Very Important Persons (VIPs) and their crew/team may be subjected to access control and exit procedure in exceptional cases.

10. Handling of visitors

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

(b) When a visitor arrives at the security main reception area 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 security officer will accredit the visitor with the access card that will be displayed visibly at all the times whilst in building.
Visitors found in the building shall be requested to produce their visitor`s cards, failing which, they shall be requested to vacate the premises, should they refuse to do so, the Trespass Act 6 of 1959 shall be applied.

All Visitors entering the building of Sedibeng District Municipality shall use the main entrance and pass through the designated reception for necessary security checks, where the normal access control procedure will be followed. All visitors shall park at the parking bays which are clearly reserved for visitors.

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

(d) No visitor will be allowed in the work station/ areas.

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

(f) In the event the visitors are a group of people attending a workshop or meeting, the host must inform the Security Manager in writing and compile a list of all visitors to attend to that effect submit it to the Security Manager as soon as possible.

(g) The reason for this practise shall be to ease unnecessary pressure at access point and to ensure that everybody is properly registered before entry is gained.

11. Cameras

(a) No cameras that are carried by visitor's area allowed into the building occupied by SDM.

(b) Journalists with cameras visiting the building of SDM on official duty will be allowed to specific area after positive identification and confirmation of invitation by host.

12. Firearms

(a) The employees are not allowed to carry firearms during their official duties, see (Firearms Control Act 60 of 2000).

(b) In case of the private person, the owner of the firearm will lock the firearm in the gun safe provided at the entry points before entering the premises of SDM.

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

(d) In terms of sec 3 of Access to Public Premises and Vehicles Act 53 of 1985, the members of South African Police Service, National Intelligence Agency, South African National Defence Force and Hawks are exempted from both access and exit control if they are in the building to execute their official tasks.

13. After Hours Control

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

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

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

(d) The employee who has required services from contractors shall supervise and be responsible for contractor's movement while in the building and report any irregularity to the Security Manager.

14. Standard Operating Procedures

ACCESS CONTROL PROCEDURES APPLICABLE AT ACCESS POINTS

7.1 All access points (gates and entrances) must be strictly controlled and be equipped with specific written post orders which define the responsibilities of security personnel posted at the specific post, the authorized access of persons (employees, visitors, contractors, deliveries, etc.), vehicles (employee and visitor cars, etc.), and items (laptops, office furniture etc.) into and out of the facility at the specific access point.

7.2 Warning signs such as the following must be posted (and be highly visible) at all access points where they may be relevant:

- *"Restricted Area"*
- *"Authorized Personnel Only"*
- *"Firearm Free Zone"*
- *"Identification Checkpoint"*
- *"Entry Constitutes Consent to Search of Person & Vehicle for Illegal Items and Weapons"*
- *"The Control of Access to Public Premises and Vehicles Act is applicable at these Premises".*

7.3 Security officers posted at pedestrian gates and entrance must:

- *stop and challenge all persons requiring access or egress;*

- *record their personal information in the appropriate registers (e.g. visitors);*
- *inspect their access cards; and*
- *search any boxes, briefcases or other items for illegal items.*

7.4 Employees must present their access cards to the security officer upon entrance and exit and wear their cards at all times while present in the facility.

7.5 All visitors (clients, service providers, contractors, etc.) must be stopped at the gate or entrance, their visit confirmed with the host, a visitor access card issued, visitor register completed and any containers opened and inspected for illegal / prohibited items. No privately owned vehicles must be permitted inside (Head Office) the facility (access must be restricted to the relevant parking or delivery areas).

7.6 ACCESS CONTROL PROCEDURES APPLICABLE TO VISITORS

7.6.1 <u>Categories of Visitors</u>

7.6.1.1 Official VIP's as determined /prescribed by management.

7.6.1.2 Official visitors (for official purposes – attending of meetings, etc.). Ad hoc contractors, electricians, technicians, etc. are included, with the exception of those mentioned in par. 7.6.1.3 below.

7.6.1.3 Consultants and contract / maintenance personnel (private companies) which are/were contracted on a permanent basis, and have been vetted for this purpose.

7.6.1.4 Non-official visitors (family members, friends or acquaintances of employees).

7.7.1 Access procedures for different categories of visitors

***Official VIP's**.*

The hosts must arrange for the reception and departure of the VIP's. All instructions from Management and Security regarding such a visitor has to be complied with and strictly adhered to. Any assistant or helper accompanying the VIP has to be provided with a visitor's card for record purposes. The VIP has to be made aware that such an assistant/helper has to accompany him/her constantly and also leave the building with him/her.

***Official Visitors**.*

This category of visitor (as described above) must report to the access control point, goes through all applicable access control procedures (as described in par 3. above) and be escorted to the venue of the meeting, workplace, etc. For this purpose the host is responsible to meet this visitor at the access control point and ensure that the visitor is accompanied /escorted for the full duration of his/her presence on the premises.

Permanent Consultants / Contractors/Maintenance Personnel.

This category of vetted visitors (as explained above) may be issued with permanent access cards; which must be programmed to provide restricted access privileges only. Escorting is not essential, although the security zones to which they may have access must be strictly controlled and monitored by security personnel.

Family members, friends or acquaintances.

Such persons may only be admitted to a waiting room/interview room at reception if not needed for official purposes. Family members, friends or acquaintances are allowed into facility offices for not more than two hours without sound motivation

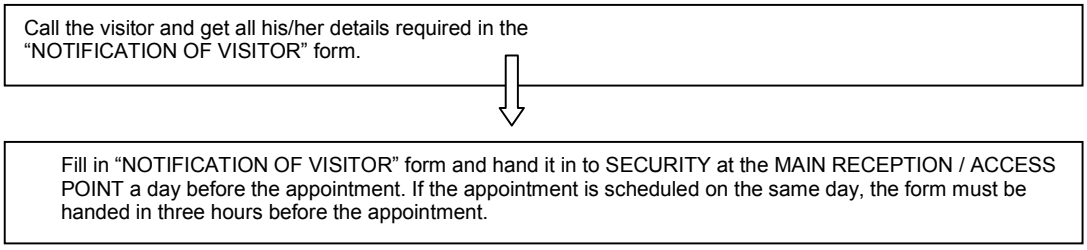
Children under the age of 11 years.

Children under the age of 11 years will be allowed into the offices, after obtaining approval from the Security Officer. This will only be allowed in EXCEPTIONAL CIRCUMSTANCES (e.g. where a sick child has to be taken to the doctor and an appointment cannot be secured outside working hours).

Children over the age of 11 years.

Children older than 11 years will be allowed into facility offices for not more than two hours. They must wait to be attended to by their parents at reception. Chairs will be placed in the reception area for this purpose. Children should not be left alone at reception for more than two hours.

7.7.3 PROCEDURE TO FOLLOW WHEN EXPECTING A VISITOR (EMPLOYEES)



Should employees require meeting facilities, it must be indicated in the form in the section "MEETING FACILITIES BOOKING", and select according to requirements. Such bookings must be communicated (and the form must be handed in) before 15:00 a day before the meeting for proper facilitation of bookings.

- All visitors must be collected at the MAIN RECEPTION / ACCESS POINT by the employee hosting the meeting.
- The visitor must be escorted by the employee hosting the visit at all times while on the premises.
- The visitors' access card will be linked to that of the employee hosting the visitor.
- All visitors must be escorted back to the reception to unlink the cards and the employee must sign that the visitor has been returned.

8.1 FACILITY ACCESS CARD SYSTEM

Each person authorized to work within the facility must be issued an access card for entrance and exit purposes.

The access card program are managed in conjunction with HR by a computer-based system which functions with biometric confirmation or proximity access cards, assigns zones of access, permits or denies a person's access into a specific zone and records this activity into a database.

8.1.1 The front of the employee access card must have:

- *a colour photo;*
- *the employee's name and signature;*
- *pay number;*
- *the employee's position; and*
- *an expiry date.*

8.1.2 The back of the access card must note:

- *the employee's date of birth;*
- *assets number (laptop) if applicable*
- *signature of the Security Manager.*

8.1.3 Each employee's access card must be programmed (by the security officials assigned with this specific responsibility) and be linked to HR system to allow access to specific zones, this being based on his or her job or position requirements.

8.1.4 Employees who have forgotten or lost their cards must be issued a temporary card for the day or while a new card is being prepared at employees R50.00 fee.

Visitor cards must:

- *be for one-day use;*
- *disposable;*
- *note the name of the visitor;*
- *identity document or passport number;*
- *indicate the area or zones authorized to be visited;*
- *contain the date and time issued.*

Non-employees who temporarily or frequently work at the facility (such as contractors, clients and government representatives) must be issued a card similar to the employee access card (but of a different colour or design) after being subjected to an accreditation process. A permanent record of the issue of all non-employee cards (with the captured data) must be maintained for at least 2 years after expiry.

It is important that the card be deactivated and retrieved when an employee or temporary employee / contractor no longer has authorized access rights (dismissed, resigned, etc.). Security must therefore be notified of any resignations or dismissals by HR before the person leaves the facility (see "Employee Exit Procedures" for the protocol to be followed).

9.1 ENTRANCE AND EXIT GATES

9.1.1 The number of facility entrances and exits must be limited to a minimum and their purposes specifically defined. There must be separate gates for pedestrians and vehicles. Likewise, there must be separate gates for the entrance and exit of those vehicles driven by employees, service providers, clients and visitors. Physically, the gates must be constructed so as to meet the same minimum standards as the perimeter fence. These gates must lock with heavy-duty security padlocks. Keys to the gates must be controlled by security personnel.

A security gatehouse must be located at each primary access point. The gatehouse and must be equipped with the following basic items:

- *fire extinguisher;*
- *first aid kit;*
- *flashlight;*
- *belly scope;*
- *power points;*
- *communication equipment (radio, telephone);*
- *rain protection equipment;*
- *vehicle and visitor gate register;*

- *occurrence book;*
- *after-hours register;*
- *equipment control registers;*
- *emergency telephone notification list;*
- *security post orders;*
- *relevant contingency plan;*
- *screening equipment (x-ray machines, metal detectors);*
- *security booths and turnstiles at pedestrian entrances;*
- *CCTV surveillance cameras;*
- *panic alarms.*

10.1. Control Room Operations

The functions of a security control room should include and but not restricted:

Monitoring and operating of the following electronic security systems and equipment;

- *CCTV surveillance and detection equipment;*
- *Intruder alarms;*
- *Panic alarms;*
- *Electronic access control systems;*
- *Fire detection and control systems;*
- *Radio and telecommunication equipment;*
- *PA system;*
- *Evacuation system;*
- *Security lighting;*
- *Back-up power for security systems (UPS,generator);*
- *Back-up of electronic security system information(e.g. CCTV);*
- *Controlling of all the key control functions (including the issue of access contol cards);*
- *Controlling of all contingency plans, action plans and associated procedures;*
- *Central communication point for all aspects relating to the security function;*
- *Record keeping and planning of security related events;*
- *Firearm control;*
- *Initiating response to alarm and emergency situations (see attached ERP-Emergency Responsive Procedures);*
- *Contact with ERAC- Emergency Responsive Action Committee (e.g. Fire Department, SAPS, Disaster Department and Community Services).*

The following information sources should be available in the security control room:

- *Security policy of SDM;*

- *Security plan of SDM (Directives' and SOP);*
- *Site and floor plan of SDM;*
- *Contingency plans (including action plans for all contingencies and evacuation plans);*
- *OHS policy, procedures and directives;*
- *Equipment operating procedures.*

The physical structure of the control room should have the following characteristics:

- *Situated on the ground floor or in the basement of the building;*
- *Solid double brick wall construction, concrete roof construction;*
- *Bullet proof widows;*
- *Double doors consisting of a solid wooden interior door fitted with a high security lock*
- *Vault/walk-in-safe for storage of firearms and other valuable/sensitive assets (e.g. back- up media) and*
- *Air conditioning.*

Recommended / Not Recommended

…… ……..
Executive Director: Corporate Services *Date*
Adv Mosotho Petlane

Approved / Not Approved

....
Municipal Manager *Date*
Mr. Yunus Chamda

SECURITY DIRECTIVE

TO: ALL EMPLOYEES	FROM: DIRECTOR:FACILITIES MANAGEMENT DIRECTORATE REF : SECURITY MANAGER
CC: MUNICIPAL MANAGER ALL EXECUTIVE DIRECTORS CHIEF FINANCIAL OFFICER ALL PMT,s OFFICES	DATE: 27 SEPTEMBER 2010

SECURITY DIRECTIVE 04: File Nr 8/2/2/84-2010

Re: VETTING/PERSONNEL SUITABILITY CHECKS/PRE-SCREENING

The objective of this directive is to describe the minimum security measure 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.

15. Security vetting

Vetting determines the integrity, reliability, trustworthiness and loyalty of a person towards the Republic of South Africa and the constitution.

- *The Municipal Manager shall ensure that personnel with access to classified information are vetted.*

- *The Municipal Manager and ED: Corporate Services in consultation with the Security Manager shall determine the level of security clearance for each applicant.*

- *The Security Manager is delegated with the responsibility of ensuring the adherence of National Strategic Intelligence Act and Minimum Information Security Standards is practical.*

- *Every employee who has access to classified information must be vetted. The Security Manager with assistance of Sedibeng District Municipality Security Committee shall from time to time identify critical areas with regard to flow of information and recommend to the Municipal Manager who must be vetted or re-vetted.*

16. Personnel Suitability Checks

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

(b) Permanent appointment of the prospective employee will depend on the outcome of the results of vetting.

17. Security screening of consultants/contractors

(a) Sedibeng District Municipality must indicate in advance on the documents to the Bid Evaluation and Bid Adjudication Committee or Contractors the security implications that should be taken into consideration/account when they perform their duties. A reason must be given for the inclusion of a clause in the tender document that indicating the degree of level, as well as the clause to ensure the maintenance of security during 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 services to Sedibeng District Municipality, must be subjected to record checking as the interim measure before they can be cleared by 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.*

(b) Acceptance of the tender is also subject to the condition that the contractor will implement such security measures as the safe performance of the contract require.

(c) The security responsibilities of the contractor must be determined by the Municipal Manager, Chief Financial Officer and Security Manager.

18. Visits abroad

(a) In the event where an official with clearance travels abroad, the ED: Corporate Services or a person assigned for the preparations must keep record of such

visits. The appropriate form must be completed and submitted to the Security Manager.

(b) When officials are travelling abroad, they must be on the guard against any attempt by a foreign intelligence to recruit them. If a person is approached, he /she must immediately on returning, report the fact to Municipal Manager and Security Manager and such information will be conveyed to the NIA.

While travelling, officials must maintain a low profile and be careful not to place themselves under compromising situations.

Recommended / Not Recommended

……. **…….**
Executive Director: Corporate Services ***Date***
Adv Mosotho Petlane

Approved / Not Approved

…….. **……**
Municipal Manager ***Date***
Mr Yunus Chamda

SECURITY DIRECTIVE

TO: ALL EMPLOYEES	FROM: DIRECTOR:FACILITIES MANAGEMENT DIRECTORATE REF : SECURITY MANAGER
CC: MUNICIPAL MANAGER ALL EXECUTIVE DIRECTORS CHIEF FINANCIAL OFFICER ALL PMT,s OFFICES	DATE: 29 SEPTEMBER 2010

SECURITY DIRECTIVE 05: File Nr 8/2/2/85-2010

Re: Security Administration and Organization

The objective of this directive is to ensure the efficiency and effectiveness of security programs, which must be able to administer within the particular mandates and according to Sedibeng District Municipality's priorities, budget, and organizational cultures and environments .These principles are recognised by the MISS at the same time to respond to specific concerns and other conditions by advocating a risk management approach to security.

Security Administration

(a) *The Municipal Manager, Executive Director: Corporate Service, Director: Facilities Management Directorate and Security Manager must ensure that Security Unit implement an effective security program that is an integral part of the overall institutional goals and objectives and that it meets the requirements of applicable national legislation and Minimum Security Standards (MISS).*
(b) *Ensure that security measures applied for protection of sensitive information, assets and employees are based on a risk management methodology and MISS.*
(c) *Ensure that effective security awareness and training programs are in place.*
(d) *Ensure that possible breaches of security are investigated, that action is taken to minimize loss, and that appropriate administrative or disciplinary action is taken, if warranted.*
(e) *Ensure that security requirements are included with other requirements in contracts when they involve access to sensitive information and assets.*

Security Administration Implementation Plan

- *Develop and implement security policy and security directives for municipal internal security management.*
- *Management and monitoring of security service provider contract and performance.* ***Adhoc security service from all Clusters***
- *Security provision during the institution's events: all employees should forward a formal written memo to Security Manager signed by the relevant MANCO member or as delegated five (5) working days before the date of the event;*
- *Approved memo should indicate number of security personnel requested, vote number, budget available for Security Manager to deduct charge out fee against the relevant vote number.*
- *Security Manager to facilitate and co-ordinate the following:*
  - *Security Committee*
  - *Parking Committee*
  - *Emergency Response Action Committee.*
- *To conduct security awareness and training programs twice a year for the all the employees.*
- *SDM Security personnel must attend security course provided by NIA for minimum security competency compliance.*
- *The Municipal Manager, Executive Director :Corporate Services,Director:Faclities Management Directorate and Security Manager must implement minimum physical security measures i.e. access control, camera's are functioning for security breaches investigations, control room in compliance with minimum standard.*

Security Organizational structure

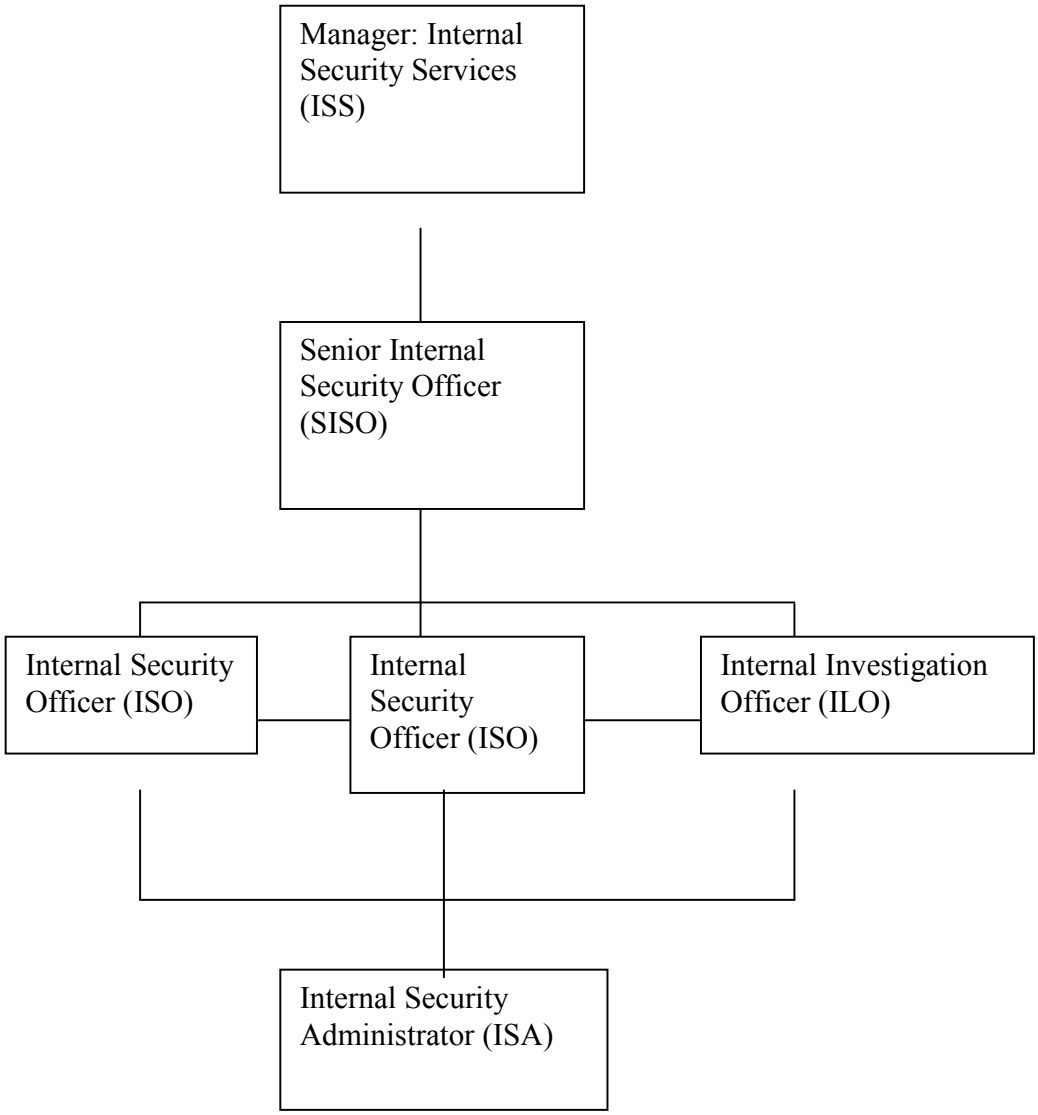
- *To ensure that security management approved structure and ergonogram is in place (see attached proposed security ergonogram).*
- *The security organizational structure must encompasses responsibility for the overall management of SDM security programs, including administrative security functions, information security, physical security ,personnel security ,information and communication technology security, business continuity planning, and that meets the needs of SDM.*

Recommended / Not Recommended

....
Executive Director: Corporate Services *Date*
Adv Mosotho Petlane

Approved / Not Approved

....
Municipal Manager *Date*
Mr Yunus Chamda


Manager: Internal Security Services (ISS)
Senior Internal Security Officer (SISO)
Internal Security Officer (ISO)
Internal Security Officer (ISO)
Internal Investigation Officer (ILO)
Internal Security Administrator (ISA)

SECURITY DIRECTIVE

TO: ALL EMPLOYEES	FROM: DIRECTOR:FACILITIES MANAGEMENT DIRECTORATE REF : SECURITY MANAGER
CC: MUNICIPAL MANAGER ALL EXECUTIVE DIRECTORS CHIEF FINANCIAL OFFICER ALL PMT,s OFFICES	DATE: 27 SEPTEMBER 2010

SECURITY DIRECTIVE 06: File Nr 8/2/2/87-2010

Re: TECHNICAL SURVAILLENCE COUNTERMEASURES

The objective of this directive is to ensure that a specific office, boardroom or other facility that will be or is frequently used for sensitive discussions can be used without the possibility of the proceedings being intercepted or monitored. Secondly, to ensure long term sterility by requiring proper security measures to such facilities as precondition for the service.

Employee's responsibilities

(a) Sensitive areas must always be under responsible control and comply with the Minimum Information Security Standards.

(b) Effective access and key control to sensitive areas must be maintained before and after TSCM inspection to ensure long term protection.

(c) Vulnerable areas must be identified in sensitive discussion areas and report to the Security Manager.

*(d) Maintenance/installation/construction/cleaning in sensitive discussion areas must **always** be done under the supervision of security personnel or an employee of the institution.*

(e) Records must be kept of all maintenance and installation personnel activities and all other visits by outsiders to sensitive areas.

(f) Requests for TSCM services must be forwarded through the allocated security advisor of the institution. Requests may under no circumstances forwarded directly to NIA TSCM unit.

(g) Suspicions of electronic surveillance should never be discussed in the direct area of concern. This includes requesting a TSCM service by telephone to or questioning NIA investigators about sweeping, bugging or tapping in the target or adjacent areas.

(h) Verbal requests must be followed up by means of a written request stating the reason for concern.

(i) Security Manager must assist NIA TSCM team to effectively execute its function by facilitating access to targeted areas and providing all pre survey information.

(j) Telephones and cellular phones must never be used for sensitive conversations.

(k) Unsecure telecommunication lines must never be used to communicate sensitive information (SACSA encryption devices be used to facilitate the need).

(l) Agendas for meetings stating sensitive points of discussion must be properly handled and secured in order to comply with the need-to-know principle and to prevent non participants to know well in advance what is going to be discussed. The same applies to the travelling of the Executive Mayor, the Speaker and Municipal Manager, Executive Directors and Chief Financial Officer.

(m) Electronic equipment such as cellular phones and laptops computers should not be allowed in sensitive discussion areas. All electronic equipment such as pagers, electronic diaries and pocket calculators can be modified into transmitters. Safekeeping should be arranged for such equipments and we should provide our own electronic equipment that can be utilized for electronic presentations.

(n) Employees must be on the look-out for signs of tempering in their offices and/ or unusual behaviour which may be an indication of an electronic surveillance operation and report immediately to the Security Manager.

(o) Any signs of efforts to gain illegal or surreptitious entry to TSCM secured areas must be reported immediately to the Security Manager.

(p) Any sensitive activity in areas of suspicion or concern must be stopped immediately or cancelled.

(q) Suspicion of possible covert surveillance installation or physical discoveries by employees or the NIA sweeping team should be kept confidential-further investigation may be jeopardized if it is made public knowledge.

Recommended / Not Recommended

.....
.....
Executive Director: Corporate Services ***Date***
Adv Mosotho Petlane

Approved / Not Approved

.....
.....
Municipal Manager ***Date***
Mr Yunus Chamda

ANNEXURE: A

SEDIBENG DISTRICT MUNICIPALITY EMERGENCY MANAGEMENT PLAN AND EVACUATION PROCEDURES

NO	EMERGENCY PROCEDURES
1	Emergency Contact Numbers
2	Client Contact Numbers
3	Emergency Contingency Plan (Where does security staff fit in?)
3.1	Fire
3.2	Flooding
3.3	Injury
3.4	Evacuation
3.5	Telephonic Bomb Threat
3.6	Intrusion
4	**ADDITIONAL TASKS/INFORMATION**
4.1	Faulty Lifts
4.2	List of Emergency Teams
4.3	Machinery and Client Equipment
4.4	Site Plan
5	**MANAGEMENT INSPECTIONS/EVALUATIONS**
5.1	Site Induction/O.J.T. Record
5.2	Monthly Inspection audit/Record
5.3	Site Inventory
5.4	H.Q. Site Visit Form
5.5	Monthly Report

MODULE 11	EMERGENCY PROCEDURES	PAGE 1 OF 16	DATE: 01/08/2010

11.1 CONTACT NUMBERS Telephone Number Speed Dial

S A Police	10111
Fire Department	10177
Ambulance	10177
Flying Squad	10111

Futuris Guarding Systems (Pty) Ltd

Head Office	(016) 362-2772
Control Room Meyerton	(016) 362-2772
Control Room Sedibeng	(016) 450-3155
Company Directors	
Mr. Rian van Zyl	082 854 8057
Mr. Paulos Mamuvila	082 386 8762
General Manager	
Mr. Jaco Smith	072 144 1441
Operations Manager	
Mr. Andries van Tonder	082 714 3905

11.2 SEDIBENG DISTRICT MUNICIPALITY

Internal Security Manager	
Mrs. Tilly Hlongwane	079 699 4417
Senior Security Supervisor	
Mr. Norman Mabula	083 630 6706
Other	078 329 3223

MODULE 11	EMERGENCY PROCEDURES	PAGE 2 OF 16	DATE: 01/08/2010

	EMERGENCY PROCEDURES		

SECTION 1

1. AIM:

1.1 To provide procedures, equipment and manpower in the event of an emergency arising at or near Sedibeng District Municipality.

1.2 To ensure the orderly and efficient transition from normal to emergency operations and to maintain the continuity of production during periods of social or industrial unrest.

SECTION 2

2. IMPLEMENTATION AUTHORITY

The Emergency Plan may be activated either wholly or partially by any Executive Director or Futuris Guarding Systems Site Manager.

In any decision to activate the emergency plan cognisance must be taken of :-

2.1 The nature and extent of possible threat to life and property.

2.2 The probable course events will take.

SECTION 3

EMERGENCY CONDITIONS

3. Precautionary phase

Precautionary measure, as listed in section 4, may be activated when the following conditions apply:-

3.1 Social Unrest

Social unrest, either on a local or national scale, is imminent or is current but is not yet affecting Institution operations.

3.2 Threats

Threats are made to damage or otherwise prejudice the operating capabilities of Sedibeng District Municipality.

3.3 Sabotage

An act of sabotage or arson is committed against Sedibeng District Municipality.

3.4 Active Phase

3.5 Industrial threat

Strikes are held or employees of the Institution take industrial action or the work force is prevented from attending work due to intimidation or subversion.

3.6 Rioting
There is unrest in the immediate area of the plant, which is either affecting or is about to affect the safety of personnel and assets.

3.7 Sabotage

Acts of sabotage or terrorist attacks are prevalent.

3.8 Disaster
The plant is threatened by serious fire or natural disaster.

SECTION 4

4. PRECAUTIONARY PHASE

4.1 In the event of a disturbance or an attack on Sedibeng District Municipality becoming imminent, consideration should be given to implementing the following precautions following an emergency meeting of the Managers when responsibilities will be allocated.

4.2 Updating the emergency plan if this was last done more than one month previously.

4.3 Increasing liaison with police and neighboring plants.

4.4 Increasing the number of security personnel on duty.

4.5 Readying control room equipment and checking emergency communications equipment.

4.6 Readying an auxiliary power supply.

4.7 Practicing or reminding employees of evacuation procedures.

4.8 Reminding employees of rendezvous points.

4.9 Briefing emergency volunteers and teams and placing them on stand-by.

4.10 Obtaining adequate supplies of production materials and fuels.

4.11 Checking and servicing fire-fighting equipment.

4.12 Rotating or re-keying locks and padlocks.

4.13 Clearing a helicopter-landing zone.

4.14 Tightening access control and search procedures.

4.15 Psychologically preparing employees to remain on the job and to resist outside pressures
by :-

- Ensuring that good labour relations exists.

- Advising employees not to associate with troublemakers.

- Requesting employees to report all rumors.

4.16 Giving employees daily briefings immediately before or during disturbances, which are aimed at dispelling rumors and speculation.

4.17 Closing the main, gates when they are not in actual use.

SECTION 5

5. ACTIVE PHASE

5.1 Dependent on the actual nature of the emergency consideration should be given to activating the following procedures:-

5.1.1 The control post is opened and manned on a 24-hour basis.
5.1.2 All Security personnel are accommodated and fed within the plant.
5.1.3 Emergency fire, repair, rescue and security personnel and teams are placed on duty.
5.1.4 Additional protection is provided for vital machinery, fuels, flammables and non-Institution property.
5.1.5 Daily employee briefings are commenced.
5.1.6 Stringent access control measures are enforced.
5.1.7 Female employees are escorted to work, car pools are initiated, alternative transport systems are utilised, and rendezvous points are brought into use.

SECTION 6

INTERNAL STRIKES AND INDUSTRIAL UNREST

6.1 AIM

Plans of action are necessary to deal with the following manifestations of industrial unrest:-

6.1.1 Refusal to work overtime (nightshift).
6.1.2 Go slow.
6.1.3 Official (Union controlled) strike.
6.1.4 Down tools.
6.1.5 Unofficial (wildcat) strike.
6.1.6 Picketing.
6.1.7 Faction fighting/rioting.

6.2 ADVANCE WARNING

6.2.1 All means available should be used to obtain as much advance notification as possible of impending industrial action by the work force, or the spread of strikes from other factories. These should include:-
6.2.2 Effective and meaningful channels of communication between management and employees.
6.2.3 Monitoring of news programs.
6.2.4 Exchanges of information with other companies.
6.2.5 The gathering of information within the works by security staff, supervisors, the personnel department and other interested parties.

6.2.6 Briefing from Industrial Bargaining Council/SHERIFS.

6.3 ACTION IN THE EVENT OF INDUSTRIAL DISPUTES

6.3.1 Immediate liaison must be set up between the under mentioned so as to ensure both a co-ordinated plan of action and the necessary protection of personnel and assets should violence ensue:-
* Executive Directors
* Works management
* Personnel department
* Security department

6.3.2 In the event of passive industrial action, i.e. go-slow or work stoppage, the following precautions should be taken:-

6.3.3 Identifying spokesmen/ringleaders and commencing negotiations away from crowds, providing there is a return to work.

6.3.4 Avoiding provocation and confrontation at all costs.

6.3.5 Keeping the police off the property.

6.3.6 Not employing casual workmen to replace striking employees.

6.3.7 Having security staff maintain a low profile whilst monitoring employee activities and placing additional staff on standby.

6.3.8 Should the industrial action take a militant form or violence become imminent, the following steps should be considered:-

6.3.9 Requesting police assistance.

6.3.10 Permitting exit from the plant and access to the car park by both non-involved employees and troublemakers.

6.3.11 Evacuation of office staff.

6.3.12 Evacuation of entire plant.

6.3.13 Securing and guarding of:-
* Main store
* Inflammable stores
* Erection store
* Fuel pumps
* L.P. Gas
* Garage
* Transport
* Restricted workshops
* Vital machinery
* Office block
* Key cupboards

6.3.14 Bringing entire security force on to site equipped for overnight stay.

6.3.15 Utilising the services of loyal employees in the control of unruly mobs.

6.3.16 Arming security personnel in the event of danger to life or property.

6.3.17 Advising neighboring companies by using the cellular.

CONTROL CENTRE

7.1 The emergency control centre is the training centre.

7.2 The alternative control centre is the JOC at Fresh Produce Market, Vereeniging.

7.3 Personnel requirements:-
* 1 x Co-ordinator (senior Security Officer on duty)

* 1 x Assistant

7.4 Equipment requirements:-

* 1 Cellular telephone
* Incident logbook
* List of key personnel addresses, telephone numbers and cellular phone numbers
* Site plan containing the location of the following:-
* Water mains
* Electrical mains, transformers and distribution boards
* Fire fighting equipment
* First aid equipment
* Safety equipment
* Manifolds and LPG storage areas
* Compressors
* Fuel and inflammables
* Emergency exits
* Employee distribution
* Assembly places and evacuation routes.
* Area map showing police and municipal boundaries and employee rendezvous points.
* List of volunteers for emergency duties
* List of important external telephone numbers
* Torches
* Loud hailers
* Handcuffs

SECTION 8

EVACUATION PROCEDURES

8.1 Administration Block

For emergency purposes the office block is divided into four control areas, each having it's own exits. Two area Marshals have been designated for each area as follows:

8.1.1 Area No. 1

Marshals:

8.1.2 Area No. 2

Exit:

Marshals:

8.1.3 Area No. 3

Exit:

Marshals:

8.1.4 Area No. 4

Exit:

Marshals:

8.2 Evacuation Routes

Evacuation routes to be used will depend on the nature and extent of the emergency. However, it is anticipated that staff would be evacuated to one of two assembly areas as follows.

8.2.1 Route 1
Via the main gate.

8.2.2 Route 2
Via the route shown on annexure 'D' to the assembly area indicated within the yard.

8.2.3 The appropriate route and assembly area will be selected by either the Executive Director or the Security Chief.

8.3. Evacuation Procedures

Marshals, upon receipt of evacuation instructions are responsible for:

8.3.1 Ensuring that all persons, including visitors, in their area are accounted for and evacuated.
8.3.2 Checking that windows are closed in the event of a fire, and that all electrical equipment is switched off.
8.3.3 Carrying out a brief search of each office or other room in the presence of the occupants, where possible, and reporting any suspicious containers or packages to security staff.
8.3.4 Grouping staff/visitors from their areas of responsibility together at the selected assembly area whilst waiting further instructions.
8.3.5 Ensuring that no personal vehicles are taken out of the plant by evacuated personnel.

8.4. Sedibeng District Municipality Evacuation Procedures

8.4.1 Implementation

8.4.1.1 In the event of a total evacuation of Sedibeng District Municipality being ordered this will be signaled by the hooter being activated as a siren, i.e. the hooter will be switched on and off giving it a rising and falling note.
8.4.1.2 Should a partial evacuation of the Works be ordered instructions will be passed to production departments either by telephone or word of mouth by Management as indicated in Annexure "A".
8.4.1.3 Where a partial evacuation affects non-productive departments, the relevant instructions will be passed by either telephone or word of mouth by Management as indicated in Annexure "B".

8.4.2 Evacuation Routes

In the event of total evacuation of the plant being ordered, personnel will make their way to the assembly area in the Institution car park. In order to avoid congestion at the main gate, which could delay the arrival of emergency services as well as cause possible injuries to personnel, the plant will be evacuated along the three routes as indicated below.

8.4.3 Partial Evacuation

Should a partial evacuation of the premises become necessary or should it be considered that the car park is not suitable as an assembly area for any reason, then evacuated personnel should

make their way by the most direct route to the assembly area within the works as indicated on Annexure "I".

8.4.4 Implementation

8.4.4.1 On hearing the evacuation siren, supervisors are responsible for effecting the evacuation of their workforce and any visitors in as quiet and orderly a fashion as possible, and along the allocated routes.
8.4.4.2 Machinery and electrical equipment must be shut down and a search should be carried out, in the event of bomb scare, for any suspicious packages or containers, which must be reported directly to security staff.
8.4.4.3 Employees must not be permitted to visit the canteen/changing rooms during the course of the evacuation.
8.4.4.4 Supervisors should keep their personnel in a group and should account for their workforce as far as is possible.
8.4.4.5 Employees should walk not run along the designated evacuation routes and should wait at the assembly area for further instructions.
8.4.4.6 Motorcycles, bicycles or vehicles may not be used when evacuating the site.
8.4.4.7 Once the return to work instruction is received, all employees should return by the most direct route to their work places.

8.4.4.8 Hourly paid personnel must give their employee numbers to security staff at the gate when returning to work.

8.5. Security Department

Action in the event of Evacuation

8.5.1 In the event of a total evacuation of Sedibeng District Municipality being necessary, the Duty Security Officer will arrange for the evacuation siren to be sounded from one of the following points:
* Security Office
* Reception

8.5.2 On hearing the evacuation signal, or on being informed that evacuation of the plant is to be effected, security personnel on duty will act as follows:

8.5.2.1. The senior security officer will make immediate contact with his Security Manager.
8.5.2.2 The Security Manager will advise office area marshals of the evacuation.
8.5.2.3 Security personnel on duty at the gates will turn away all visitors and vehicles, other than members of the emergency services and their transport.
8.5.2.4 Patrolling staff will be advised of which areas are to be evacuated if the evacuation is not total, and will assist in ensuring that the relevant workshops, buildings or offices have been vacated.
8.5.2.5 Patrolling staff will be advised of which areas are to be evacuated if the evacuation is not total, and will assist in ensuring that the relevant workshops, buildings or offices have been vacated.
8.5.2.6 Staff on duty at the gates will close them once evacuation is completed, but will remain at their posts unless instructed otherwise.
8.5.2.7 Any suspicious articles or containers that are located or reported will not be touched and must be reported to the security manager without delay.

8.5.2.8 The senior security officer is to ensure that the employee numbers of all hourly paid personnel are recorded at the main gate following an instruction being given to return to work.

SECTION 9

First Aid

9.1. The location of First Aid boxes throughout the premises is shown on the emergency site plan.
9.2 A Institution vehicle is reserved for the transportation of injured personnel during the day and at night.

SECTION 10

RENDEZVOUS POINT

10.1 Should access to the plant by employees be prevented by roadblocks, rioting or any other cause, personnel may be pre-warned to assemble at the following point:

SECTION 11

EMERGENCY TELEPHONE NUMBERS

Ambulance	- (016) 440 1000
Civil Defence	-
Court Helicopters	-
Private Medical Clinic	- (016) 440 5000
Electricity	- (016) 422 1656/ 455 5487
Emergency Reaction Service	-

FIRE BRIGADE

Meyerton	- 101777
Vereeniging	- 101777
Vanderbijlpark	-101777
Heidelberg	-101777
Sebokeng	-101777

HOSPITALS

Meyerton	-
Vereeniging	- (016) 950- 5000
Vanderbijlpark	- (016) 341-6000
Heidelberg	- (016) 930- 1100
Sebokeng	- (016) 930-3000

POLICE

Meyerton	- (016) 362-0126
Vereeniging	- (016) 450-2080
Vanderbijlpark	- (016) 910-9000
Heidelberg	- (016) 341-2570
Sebokeng	- (016) 988 1820/4

BOMB SQUAD

Flying Squad - 10111

SEDIBENG DISTRICT MUNICIPALITY

SECTION 12

12.1 FIRE BRIGADE

12.1.1 Sedibeng District Municipality falls under the Gauteng Provincial Government.

TELEPHONE : _____

Lapsed times for arrival on site following a call-out are:

Clear road conditions	:	minutes
Heavy traffic	:	minutes

The _____ Fire Brigade will be supplied with a site plan of the Institution containing all necessary information.

12.2 FIREFIGHTING EQUIPMENT AND PRECAUTIONS

12.2.1 Fire Alarm

The alarm signal for a serious fire will be the continuous sounding of the institution hooter.

Hooter activation points are:

To be determined when the tender is awarded

12.2.2 Fire Teams

12.2.3 Action in the event of a fire

Departmental fire officers are responsible for the putting out of fires in their areas of responsibility and taking control of personnel at the scene.

In the event of a serious fire, the Departmental Fire Officer responsible for the area concerned will activate the fire alarm.

Departmental Fire Officers will report to the scene of any serious fire on being alerted by the alarm and will form a team to extinguish the fire.

12.2.4 Control

The Senior Departmental fire Officer present will take charge at the scene of the fire and direct all fire control operations, including any necessary evacuation of the area, until the arrival of the Fire Brigade.

12.2.5 Manpower

A list of Departmental Fire Officers appears at Annexure “A” to this section. Additional trained employees are listed under Section 19.

12.2.6 Fire Instruction

General instructions for action to be taken in the event of fire are posted on all notice boards. A copy is attached at Annexure “B” to this section.

The responsibilities of Departmental Fire Officers are attached as Annexure “C” to this section.

Duties of Departmental Fire Officers

12.4.1 The co-ordination of personnel and resources in extinguishing fires in their areas of responsibility.
12.4.2 To report to the scene of and assist at any serious fire outbreaks on the sounding of the fire alarm. (Continuous sounding of the institution hooter).
12.4.3 The carrying out of weekly inspections of fire appliances in their areas of responsibility.
12.4.4 Ensuring that fire appliances are always accessible and not blocked by waste or production materials.
12.4.5 The policing of non-smoking areas and the reporting of offenders.
12.4.6 Ensuring that safety precautions for the prevention of fires are understood and acted upon.

SECTION 13

S.A.P.S. AND S.A.N.D.F.

13.1 The South African Police have a strength of approximately (??) men at _____ police station. In addition to this, they can call on an additional unit of approximately (??) men who are used on consolidated patrol and stand-by duties in the surrounding areas. However, this manpower would be rapidly dissipated in a large-scale disturbance.
13.2 Should local forces be unable to contain an outbreak of rioting additional police and army manpower could be called in from other parts of the Province and from Pretoria. Neither the S.A.P.S. nor the S.A.N.D.F. can give any guarantee of protection for individual companies other than national key points.

CIVIL DEFENCE

14.1 Civil Defence is a co-coordinating body, which is able to marshal all available resources within a community to cope with and overcome a disaster or state of emergency, i.e.
* Saving lives
* Protecting property
* Maintaining essential services

14.2 There are Civil Defence Field Officers at every Fire Station.
14.3 Civil Defence maintain a fully equipped control room in the city centre and are in immediate contact with all emergency services.

TELEPHONE NO. -

SECTION 15

15.1 SITE PLAN
The following information is recorded on site plans in this section:
15.2 INFLAMMABLES STORES AND FUEL
15.3 L.P. GAS STORAGE AND MANIFOLDS
15.4 VITAL MACHINERY
15.5 FIRST AID EQUIPMENT
15.6 EMPLOYEE DISTRIBUTION

SECTION 16

16.1 ALARM SIGNALS

16.1.1 Institution Evacuation

The institution hooter will be activated as a siren, i.e. it will be switched on and off giving it a rising and falling note.

16.1.2 Fire

The institution hooter will be activated on a continuous note for several minutes.

SECTION 17

DISASTERS AND MAJOR ACCIDENTS

17.1 RADIATION

17.1.1 Should an isotope container become damaged, refuse to open or close or if the nuclide is considered to be insufficiently shielded for any reason, it is the duty of the technician in charge to:

17.1.2 Measure the dose rate.

17.1.3 Evacuate all personnel from the affected area and rope it off.

17.1.4 Advise the Futuris Guarding Systems Site Manager/Safety Officer.

17.1.5 Advise the Responsible Person. (See paragraph 1.3)

17.1.6 In the event of an isotope becoming dislodged from its container the technician in charge will:

17.1.7 Advise the Responsible Person and the Futuris Guarding Systems Site Manager/Safety Officer.

17.1.8 Locate the source with audible and visual monitors.

17.1.9 Evacuate and rope off the area.

17.1.10 Await the arrival of the Responsible Person who will assess the situation and make all arrangements for recovering the source.

17.2 Responsible Persons

To be determined.

17.2.1 In the event of neither of the Institution responsible persons being available or contactable, the following persons should be requested to assist:

To be determined.

17.3 Theft

The holder of an authority shall notify the Director-General from the Department of Health and in the case of theft notify the South African Police by telephone, telegram, facsimile or other similar rapid means of the event in question, and such notification shall be followed up within seven days by a written report.

17.4 Fire or Flood

In the case of fire, floods and similar emergencies on the premises of a holder, the relevant local authority or person or organisation that perform cleaning up or protection work be warned of the dangers associated with the group IV hazardous substance that is under the control of the holder and be advised accordingly.

17.5 EXPLOSION

17.5.1 Action to be taken in the event of an explosion due to sabotage, fire or other cause should include the following:

17.5.2 Sounding the fire alarm.

17.5.3 Calling the Fire Brigade and Police.

17.5.4 Removing injured persons from the scene.

17.5.5 Putting out any fires.

17.5.6 Evacuating and roping off the area.

17.5.7 Establishing the cause of the explosion as soon as possible and taking immediate precautions against recurrences.

SECTION 18

POST-EMERGENCY ENQUIRY

18.1 Depending on the extent of the emergency, it may well be advisable to convene an enquiry to investigate the impact of the emergency on the Institution and the effectiveness of the emergency plan.
18.1.1 the following comparisons should be made with normal periods:
18.1.2 Daily attendance of employees.
18.1.3 Production.
18.1.4 Continuity of employees/staff.
18.1.5 Damage to the plant should be assessed.
18.1.6 The effectiveness of security systems should be assessed and corrective action taken.
18.1.7 Comparison should be made with the operating capabilities of neighboring businesses during the period concerned.
18.1.8 Recognition should be given for exemplary performance.

11.3.1 FIRE
Discussed in Emergency Plan.

11.3.2 FLOODING
Discussed in Emergency Plan.

11.3.3 INJURY
Discussed in Emergency Plan.

11.3.4 EVACUATION
Discussed in Emergency Plan.

11.3.5 TELEPHONE BOMB THREAT

All bomb threats are to be treated as true.

The following action needs to be taken when receiving such a call:

a. Obtain as much information as possible concerning the caller and the alleged bomb.
b. Immediately notify Tanker Services.
c. Complete the Bomb Threat form.

During Silent Hours

Obtain as much information as you can concerning the caller and the alleged bomb.

Complete Bomb Threat Proforma Form.

Pass the following message to the SAPS:

"This is Patrolman .....(your name) speaking from Sedibeng District Municipality. I have received a telephone message that there is a bomb on site". (Give any further details that you may have obtained). Immediately contact the Site Manager, The Head of the Protection Services. Carry out any instructions that you receive from the Head of Protection Services, Sedibeng District Municipality.

11.3.6 INTRUSION

Should any unauthorised person be found in the restricted area, the following instructions will be carried out.

a. The security official will on finding the person, detain him and notify Security Manager.
b. The security official will obtain as much information as possible of the intruders.
c. Any incidents of intruders are to be fully logged in the Occurrence Book and a complete security report submitted to Head Office as soon as possible.
d. Should the security official be unable to detain the intruder, advice must be sought from the Security Manager.

12.3 SITE PLAN

To be determined.

SDM EMERGENCY RESPONSE ACTION COMMITTEE

Contents

1. INTRODUCTION

Emergency Management is the mechanism by which disastrous or potentially disastrous situations can be managed and coordinated to ensure that the normalization of life be restored and that the loss of life or potential loss of life, injury or damage to property or the environment is minimized.

This Emergency Response Plan will allow the Sedibeng District Municipality and other role players within the area to put in place mechanisms which will reduce the risk of an emergency occurring and which will allow role players to react in a coordinated fashion in dealing with emergency that may occur in the area.

The purpose of the Emergency Response Action Committee *(ERAC)* is to:

1. To establish procedures and protocol in preparation to deal with all contingencies which will:

- Prevent loss of life and or property of Sedibeng District Municipality.
- To ensure the continuity or normal Council business or operations

2. EMERGENCY RESPONSE ACTION COMMITTEE

The Emergency Response Advisory Committee will advise the Municipal Manager on matters pertaining to emergency responses and it is through this committee that the emergency Management Plan **(See attached draft plan)** will be effected according to circumstances.

- Chairperson : Director Facilities Directorate
- Deputy Chairperson: Security Manager
- Deputy Chairperson: Director Community Services
- Fire & Rescue Management :Director Ops Fire
- Disaster Management: Assistant Logistics & Support
- Emergency Response Co-ordinator:Senior Security Officer
- Emergency Response Controller: Futuris SDM Sites Manager.

Additional AD-HOC Members

- SAPS
- Traffic
- EMS
- Environmental Health
- OHS
- Finance / Supply Chain Management
- HR, and
- Any other department deemed necessary.

3. FUNCTIONS OF EMERGENCY RESPONSE COMMITTEE

In compiling this Plan the following types of emergency/risks have been considered:

- Strikes, occupation and hostage
- Security (property protection, access control)
- Fire
- Evacuation
- Threats (bomb, chemicals, explosions)
- Disaster (man made, unnatural weather)
- Communications Information Technology (sabotage)
- Water and Electricity (essential services)

The measures that will be put in place will vary according to the situation but generally the action will include the following:

• Assessment of the occurrence
• Evacuation and treatment of the injured if necessary
• Fire-fighting and rescue
• Provision of emergency accommodation
• Transportation of affected people where necessary
• Crowd and traffic control
• Establishment of emergency communication points
• Restoration of essential services

3.1 ASSESSMENT OF THE SITUATION

The initial assessment of an emergency is of vital importance as it is this assessment that will determine what action is to be taken to mitigate the effects of the emergency situation. Upon being made aware of emergency the Municipal Manager will direct that an assessment of the event be made. The Municipal Manager will assign the Chairperson or in his absence the Deputy Chairperson to conduct this assessment. The assessment must be carried out as soon as possible and all relevant information must be recorded. The magnitude of the situation will dictate how such an assessment must be conducted. Having gathered the information the Municipal Manager must be informed and if the circumstances warrant it a Joint Operation Centre (JOC) must be established in order to manage the prevailing emergency/situation.

3.2 MANAGING THE EMERGENCY

In order that the emergency is managed effectively the establishment of a JOC is of paramount importance. The JOC will be manned by the Chairperson who shall have delegated authority to take decisions together with, if the circumstances so dictate, senior officials of Service Units. The purpose of a JOC is to monitor what is being done at the scene of the emergency and to convey instructions The JOC is the vital communication

core of evaluation, decision making and channelling of instructions and should be readily accessible to the personnel who will manage it.

The JOC will require the following:

• An Operations room with space for wall maps
• Adequate lighting
• Adequate seating for staff that will manage it
• Personal Computer
• Telephone line
• Radio communication

Suggested personnel to man the JOC *(*it must be borne in mind that this scenario should be adapted to suit the situation)

Name	**Position**	**Organisation**	**Phone**	**Cell**
Mr. J. Kumalo	Director Facilities MD	SDM	4403/00	0828866590
Ms. T Hlongwane	Security Manager	SDM	4412/00	0796994417
Mr. S. Tlhapolosa	Disaster management	SDM	3170	0829014310
Mr Maleho Leacwe	Community Services	SDM	3228	0828837117
Mr. N Mabula	Senior Security Officer	SDM	4416	0836306707
Mr P Niewenhuizen	Disaster management & Communication	SDM	3105	0829015726
Mr. A van Tonder	SDM-Site Manager	FUTURIS	3000	0827143905
AD HOC: If it is necessary to call upon the assistance of the SAPS, Traffic, OHS, HR, Fire and Rescue, infrastructure	As and when required			

4. ROLES AND RESPONSIBILITIES

THE CHAIRPERSON / DEPUTY CHAIR: Mr Jabu Kumalo / Ms. Tilly Hlongwane

- Comprehensive Chairperson planning is undertaken with the assistance of the ERAC and that such planning is recorded as a written Chairperson plan;
- Chairperson team leaders and emergency personnel are adequately trained to perform their duties and that all facets of the plan are practiced regularly;
- Required equipment is procured and kept serviceable and secure;
- Emergency facilities are serviceable and well maintained;

- Communication is effective and those instructions can be given to relevant personnel in any part of the complex with a minimum of delay;
- The safety of all personnel, occupants (including handicapped) and visitors are planned for in compliance with the Occupational Health and Safety Act.
- All exits, evacuation routes, location of fire fighting and first aid equipment must be prominently indicated and clearly reflected on floor plans;
- Monthly status reports are received from all Chairperson team leaders and feedback given to top management;
- Emergency situations are effective managed;
- Teams are identified according to standard Colour codes;
- Regular exercises must be kept;
- He assumes overall command during emergencies;
- Secretaries/receptionists and switchboard operators are trained to activate emergency services without delay when authorized to do so and that bomb threats checklist are kept at all telecommunication points;
- A Chairperson Operations/Control Room and alternative centre is available and equipped. A procedure to mobilise the Coordinating and Planning Committee is in place;
- Vital movable valuables, records and documents are prioritized for salvage purposes in the event of fire; etc;
- Plans are maintain, reviewed and updated regularly;
- Team leaders are appointed and their duties are delegated in writing.
- Be responsible for all matters pertaining to fire, evacuation or other emergencies in the building until the arrival of the Emergency Services;
- Be responsible for maintaining an updated list of all floor Wardens, with telephone numbers and locations within the building; the list shall be prominently displayed on each floor;
- Be responsible of ensuring that he/she and the Deputy is not simultaneously absent from the building and that the Deputy obtains all the skills required to perform as replacement;
- In order to effective perform the role, a sound knowledge of the building, the position of all fire fighting equipment and special risk areas are required;
- Ensure that all personnel know the evacuation procedure and assembly areas,
- Carry out inspections and report on any defects of fire fighting equipment and fire doors, cluttered exit routes and poor house keeping, including the careless use/storage of flammable materials and the careless use of heating appliances and other electrical equipment.

DEPUTY CHAIR: Maleho Leacwe and Fire & Rescue Management: Mr S.Tlhapolosa

- Comprehensive Deputy Chairperson planning is undertaken with the assistance of the ERC and that such planning is recorded as a written Deputy Chairperson plan;

- Deputy Chairperson team leaders and emergency personnel are adequately trained to perform their duties and that all facets of the plan are practiced regularly;
- Required equipment is procured and kept serviceable and secure;
- Emergency facilities are serviceable and well maintained;
- Communication is effective and those instructions can be given to relevant personnel in any part of the complex with a minimum of delay;
- The safety of all personnel, occupants (including handicapped) and visitors are planned for in compliance with the Occupational Health and Safety Act.
- All exits, evacuation routes, location of fire fighting and first aid equipment must be prominently indicated and clearly reflected on floor plans;
- Monthly status reports are received from all Deputy Chairperson team leaders and feedback given to top management;
- Deputy Chairperson situations are effective managed;
- Teams are identified according to standard Colour codes;
- Regular exercises must be kept;
- He assumes overall command during emergencies;
- Secretaries/receptionists and switchboard operators are trained to activate emergency services without delay when authorized to do so and that bomb threats checklist are kept at all telecommunication points;
- A Control Room and alternative centre is available and equipped. A procedure to mobilise the Coordinating and Planning Committee is in place;
- Vital movable valuables, records and documents are prioritized for salvage purposes in the event of fire; etc;
- Plans are maintain, reviewed and updated regularly;
- Team leaders are appointed and their duties are delegated in writing.
- Be responsible for all matters pertaining to fire, evacuation or other emergencies in the building until the arrival of the Emergency Services;
- Be responsible for maintaining an updated list of all floor Wardens, with telephone numbers and locations within the building; the list shall be prominently displayed on each floor;
- Be responsible of ensuring that he/she and the Deputy Chairperson are not simultaneously absent from the building and that the Deputy obtains all the skills required to perform as replacement;
- In order to effective perform the role, a sound knowledge of the building, the position of all fire fighting equipment and special risk areas are required;
- Ensure that all personnel know the evacuation procedure and assembly areas,
- Carry out inspections and report on any defects of fire fighting equipment and fire doors, cluttered exit routes and poor house keeping, including the careless use/storage of flammable materials and the careless use of heating appliances and other electrical equipment.

THE EVACUATION LEADER: Pieter Niewenhuizen

- Determine the safest evacuation routes. Such routes must be well lit at all times.

- The evacuation routes/alternatives are clearly marked on the floor plans. The primary and secondary escape routes - preferably in colour.
- Appointment of sufficient evacuation wardens and delegating their duties and responsibilities in writing;
- Training of evacuation wardens, personnel and occupants to adequate evacuation standards;
- A record should be kept of frail and handicapped personnel and occupants. Special arrangements should be made in consultation with the first aid leader for assisted evacuation;
- Evacuation plans should also cater for total evacuation of multi-story buildings. To prevent congestion along evacuation routes different floors could be evacuated simultaneously;
- Ensure that doors and windows are closed in the event of a fire and opened in the event of a bomb incidents;
- Ensure that panic is kept to a minimum when evacuating and that order is maintained throughout;
- Identification of a number of suitable evacuation assembly points, depending on the nature of the threat.
- These assembly points should be selected in consultation with security and fire leaders and must be reflected on floor plans;
- That the complex is searched following evacuation to ensure that personnel, occupants and visitors have left and that the areas are cleared;
- That orderly shutdown procedures are adhered to;
- That regular status reports are received from the evacuation wardens during and after evacuation and forwarded to the Chairperson;
- That evacuation wardens are adequately equipped to perform their duties and to ensure that they are identifiable by means of the recommended colour codes;
- That evacuation instructions are issued confidentially or in code to alleviate panic;
- Assist the Chairperson with planning and the management of actual emergencies

SECURITY CONTROLLER: Norman Mabula and Andries Van Tonder

- Direct and ensure that all rooms, offices, records storage areas rest rooms, conference rooms, and remote areas, closing doors of areas that have been searched;
- Advice staff or other persons on the floor about the emergency and requirement to evacuate;
- Discourage people from taking heavy or awkward items with them. Personal belonging only;
- As appropriate, check that all visitors and all staff on duty at the time of evacuation can be accounted for;
- Assist any physically handicapped individuals (possibly researchers) into the stairwell or other predetermined area of refuge;
- Report any persons refusing to leave or other problems to the JOC;

- Notify the JOC that the floor is "clear" and proceed out of the building;
- Ensure that basic security are up to date and carried out by the Security Service Provider;
- After any evacuation of the building ensure that SDM management is advised that all staff are accounted for;
- To ensure that all Security Personnel are qualified and trained in CPR and First Aid
- Serve as the Alternate Evacuation Coordinator; and
- Coordinate the shutdown of operation and systems within the building(s) when necessary

5. PROCEDURAL DELEGATED FUNCTIONS

It must be borne in mind that this Emergency Management Plan is an active document +circumstances. The Municipal Manager will delegate responsibility to the Chairperson and the committee to make decisions in respect of the following:

- Total evacuation
- Releasing employees
- Emergency procurement depending on the need/circumstances
- Closing of services
- Declaring of disaster
- Delegating powers on cross cutting issues

These delegated powers will be applicable to all operational offices of the Sedibeng District Municipality and includes but not limited to the following areas:

- Sedibeng District Municipality Head office
- Vaal Technorama
- Ventura
- MSDC
- Licensing offices
- Youth Centres
- Fresh Produce Market

6. COMMUNICATION

Staff should be kept informed of any Contingency/Emergency initiatives *(Attached)* the municipality intends to adopt. This could be achieved by various means e.g. meeting and correspondences. The staff and visitors must be made aware of risks and hazards and education will go a long way in minimizing the affects of a disastrous event and such an exercise should be viewed by both officials and politicians in terms of cost of dealing with an emergency can be crippling.