Victor Khanye Local Municipality

Phone: 013 665 6000
Fax: 013 665 2913
Email: info@victorkhanyelm.gov.za
Web:
http://www.victorkhanyelm.gov.za

Corner Van Der Walt Street and
Samuel Road
P.O. Box 6
Delmas
Mpumalanga
2210

Resolution

A 031/05/2017

CERTIFIED EXTRACT OF A RESOLUTION BY THE MUNICIPAL COUNCIL IN A OC MEETING HELD ON 06 JUNE 2017 IN THE COUNCIL CHAMBER, MUNICIPAL OFFICES, DELMAS

A 031/05/2017
SECURITY MANAGEMENT POLICY
(ED:CS)

RESOLVED (THAT):

1. The Security Management Policy, be approved and adopted.

2. Upon approval the policy be referred to the South African Secret Service (SASS) for legality and compliance.

*****

This is to certify that this is a true copy of the Original

Signed: _____ Date: 2018-07-11

VICTOR KHANYE

LOCAL MUNICIPALITY – PLAASLIKE MUNISIPALITEIT

DRAFT SECURITY MANAGEMENT POLICY

Policy Number: SMP - 1	Approved by Council:
Resolution No:	Review Date:

TABLE OF CONTENTS

1. Introduction

A Security Policy is regarded as a formal statement of rules through which the security of the institution is managed to ensure an effective protection of the premises, assets, personnel, technology and information assets by implementing appropriate and accurate security measures. It defines what the institution and security objectives management desires but not how these solutions are engineered and implemented. It is a document that guides management in developing effective and comprehensive security program.

It is therefore important that it should be economically feasible, understandable, realistic, consistent and procedurally tolerable and also provide reasonable protection relative to the stated goals and objectives of management. A Security Policy should define the overall security and risk control objectives that Victor Khanye Local Municipality endorses. The characteristics of a good security policy are not limited to:

- It must be implementable through specific procedures and directives or other appropriate methods.
- It must be enforceable with security tools, where appropriate and withy sanctions, where actual prevention is not technically feasible.
- It must clearly define the areas of responsibility for the different aspects of security as per MISS document; and
- It must be documented, distributed and communicated.

2. Definition of key concepts

2.1 Access Control

The process by which access to a particular area is controlled or restricted by applying effective and efficient security measures.

2.2 Classification

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

2.3 Contingency Planning

It is regarded as 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 practice thereof, in order to identify and rectify gaps in the plan, and to familiarize personnel and co-ordinators with the plan.

2.4 Computer Security

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

2.5 Communication Security

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

2.6 Declaration of Secrecy

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

2.7 Delegation

This regarded as the transfer of authority, powers or functions from one person to the other.

2.8 Document

In terms of the Protection of Information 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.

2.9 Document Security

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

2.10 Employees

For the purpose of this policy the term employees includes:

- Permanent Staff;
- Temporary Staff;
- Interns; and
- Contract staff

2.11 Information Security

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

2.12 Personnel Security

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

2.13 Physical Security

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

2.14 Premises

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

2.15 Screening Institutions

The institutions (SAPS, SSA, SASS and SANDF) that, in terms of the relationship agreement, are responsible for the security screening and vetting of persons within their jurisdiction. State Security Agency (SSA) has a legal mandate to employees within

the public service.

2.16 Security

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

2.17 Security Audit

That part of the 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 problem experienced; and encourage a high standard of security awareness.

2.18 Security Clearance

It is regarded as 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 and official (s). An official document that indicates the degree of security competence of a person.

2.19 Visitors

For the purpose of the policy visitors shall refer to the members of the public including non – staff members.

2.20 Contractors/Service Providers

Any individual or company rendering a service to Victor Khanye Local Municipality.

3. Principles

The 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 Victor Khanye Local Municipality.

The principles here are based upon the following achievable goals;

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

4. Statement of purpose

Victor Khanye Local 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 Victor Khanye Local Municipality, in South Africa and abroad includes acts of terror, 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 the 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 international environment.

The Security Policy of Victor Khanye Local 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 Victor Khanye Local Municipality rely extensively on information and communication technology (ICT) equipment as well as ICT protection measures to be complied with by employees and through the assistance of the ISO (Information Security Officer) delegated by the municipality in support to the POPI Act (definition: **PoPI Act** is to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise your personal information in any way).

The main objective of this policy therefore is to support the interest of the community we serve and Victor Khanye Local Municipality business objectives by protecting employees, information and assets and assuring the continued delivery of service throughout the Victor Khanye jurisdiction area and to South African citizens.

The policy compliments other policies of Victor Khanye Local 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.)

5. Scope

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

- Executive Mayor, the Speaker, Council Whip, the Mayoral Committee Members and all other Councillors.
- The Municipal Manager and all section 57 Managers.
- All employees of Victor Khanye Local 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 including interns and other contractual workers.
- All information assets of the Municipality.
- All intellectual property of the Municipality.
- All fixed property that is owned or released by the Municipality.
- All movable property that is owned or leased by the Municipality.

5.2 The policy further covers the following seven (7) 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

6. Legislative and Regulatory Requirements

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:

- The Constitution of South Africa, Act 108 of 1996
- Control of Access to Public Premises and Vehicle Act 53 of 1985
- Criminal Procedure Act 51 of 1977
- MISS Policy of 1996
- Trespass Act 6 of 1969
- Security Officers Act 92 of 1987
- Public Services Regulation 2001 which replaced the 1999 Regulation
- Extension of Security of Tenure Act 62 of 1997
- Fire-arms Control Act 60 of 2000
- Hazardous Substance Act 15 of 1973
- Intimidation Act 72 of 1982
- Public Service Act Proclamation103 of 1994
- National Building Regulations and Building Standards Act 103 of 1977
- National Archives and Record Service of South Africa Act 43 of 1996 (Previous short title "National Archives of South Africa" substituted by s. 19 of Act 36 of 2001)
- Protection of Information Act 84 of 1982
- Protected Disclosure Act 26 of 2000
- Promotion of Access to Information Act 2 of 2000
- National Strategic Intelligence Act 39 of 1994
- Occupational Health and Safety Act 85 of 1993
- Private Security Industry Regulation Act 56 of 2001
- POPI Act No 4 of 2013

7. Policy Statement

7.1 General

7.1.1 This policy seeks to:

- Protect the Executive Mayor, Speaker, the Council Whip, Mayoral Committee Members, all other Councillors, the Accounting Officer, section 56 managers, all employees and visitors to Victor Khanye Local Municipality against identified threats according to baseline security requirements and continuous risk management.
- To secure the information and assets of Victor Khanye Local Municipality against identified according to baseline

security requirements and continuous risk management.

- To ensure continued delivery of services of Victor Khanye Local Municipality through baseline security requirements, including business continuity planning and continuous risk management.

7.1.2 Applicability

This Policy is applicable to all employees of the Municipality, consultants, contractors and any other service provider of Victor Khanye Local Municipality. It is further applicable to all visitors and members of the public visiting premises of the municipality or may officially interact with the institution.

7.2 Compliance Requirements

All individuals mentioned in paragraph 5.1 above must comply with baseline security requirements of this policy and its associated security directives as contained in the security plan of Victor Khanye Local Municipality. These requirements shall be based on the integrated security Threat and Risk Assessments (TRA's) to the interest of the Municipality and its employees, information and assets of the Victor Khanye Local 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 Assessment 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.

7.3 Staff accountability and acceptable use of assets

7.3.1 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 Victor Khanye Local Municipality.

7.3.2 All employees of Victor Khanye Local 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.

7.4 Specific Baseline Requirements

7.4.1 Security Administration

The functions referred to in paragraph 7.3.1 above includes:

- 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 and vetting.
- Implementation, monitoring and evaluation of physical security.
- Ensuring the protection of employees and visitors.
- Ensuring the protection of information.
- Ensuring ICT security compliance. (ICT Governance and Framework)
- Ensuring security in emergency and increased threat situation.
- Facilitating business continuity plan.
- Ensuring security in contracting.
- Facilitating security breach reporting and investigations.
- Implementing Security Strategic Planning.

7.4.2 Security incident/breaches reporting and response process

7.4.2.1 Reporting

- 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/ Executive Director Corporate Services/ Executive Manager delegated to deal with secirty matters of the institution by utilizing the formal reporting procedure prescribed by the Security Breach Directive of the institution.

- 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.

- The Security Manager of the institution shall ensure that all employees are informed about procedure for reporting security

breaches.

7.4.2.2 Response

- The Security Manager shall develop and implement security breach response mechanism for the institution in order to address all security breaches/alleged security breaches which are reported.

- The Security Manager shall ensure that the Accounting Officer is informed and advised as soon as possible.

- It shall be the responsibility of the National Intelligence Structures (e.g. SSA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the Security Manager of the institution.

- 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 investigation into security breaches or alleged security breaches.

- The end results of this 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.

7.5 Information Security

Categorization of information and information classification system

7.5.1 The Security Manager with the support from the ISO 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.

7.5.2 All sensitive information must be categorized into one of the following categories:

- State Secret
- Trade Secret
- Personal Information

- Shared Information

And subsequently classified according to its level of sensitivity by using one of the recognized levels of classification:

- Confidential
- Secret
- Top Secret

7.5.3 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 labelling of classified documents.

7.5.4 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.

7.5.5 Access to classified information will be determined by the following principles:

- Intrinsic secrecy approach
- Need-to-know basis
- Level of security clearance

7.6 Physical Security

7.6.1 Physical security involves the physical layout and design of facilities of Victor Khanye Local 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.

7.6.2 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.

7.6.3 Victor Khanye Local 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 necessary entry barriers, security systems and equipment to effectively control access thereto.
- During the sitting of Council meetings the passages as well as the entire municipal building should be under hightened security. The door next to the municipal manager's offce leading to the political wing should be locked until the meeting is concluded.
- Any member of the community who is to attend any sitting of the municipality should be sitted when the meeting assumes and no late entrants [members of the community] should be allowed to enter the premises.
- Include the necessary security specifications in planning, request for proposals and tender documentation.
- Incorporate related costs in finding requirements for the implementation of the above.
- In case of a forceful entry into the municipal buildings the Municipal Manager or his senior manager (delegated/acting) should as a matter of urgency in consultation with the Security Manager liaise with the SAPS and open a case of forceful enrty/transpassing should be opened and same should be followed – up for consequnce management outcomes.

7.6.4 Victor Khanye Local Municipality will further ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms.

7.7 Personnel Security

7.7.1 Security Screening

7.7.1.1 All newly appointed employees, contractors and consultants attached to Victor Khanye Local Municipality, who requires access to classified information and critical assets in order to perform his/her functions, must be subjected to a security screening and vetting investigation conducted by the State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

7.7.1.2 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.

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

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

7.7.1.5 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 and re-vetting on a more frequent basis as determined by the Municipal Manager, based on information which impact negatively on an individual's security competency.

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

7.7.2 Polygraph Screening

7.7.2.1 A polygraph examination shall be utilized to provide support for the security screening process. All employees subjected to a Top Secret clearance shall 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 part of the person being examined.

7.7.2.2 In the event of any negative information being obtained with regard to the person being examined during the security screening investigation (all levels), such a 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 however limitations might apply.

7.7.3 Transferability of security clearance

7.7.3.1 A security clearance issued in respect of an official from other Government Institution shall not be automatically be transferable to Victor Khanye Local Municipality. The responsibility for deciding whether the official should be re-screened rests with the Municipal Manager.

7.8 Security Awareness and Training

7.8.1 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 remains security conscious.

7.8.2 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 security policy and security measures of the Office of the Executive Mayor and the need to protect sensitive information against disclosure, loss or destruction.

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

7.8.4 Regular surveys and walkthrough inspections shall be conducted by the Security Manager and members of the security component and security committee to monitor the effectiveness of the security awareness and training program.

7.9 Information and Communication Technology (ICT) Security

7.9.1 IT Security

7.9.1.1 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.

7.9.1.2 To prevent the compromise of IT system, the Municipality shall implement baseline security controls and any other additional controls identified through the security (TRA) Threat and Risk Assessment. These controls, and the security roles and responsibilities of all personnel shall be clearly defined, documented and communicated to all employees.

See Security Directive on Reporting of Security Breaches

7.9.1.3 To ensure policy compliance, the Assistant Manager ICT 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 as per Information Security Policy the municipality has in place

- Periodically request assistance, review and audits from the National State Security Agency in order to get an independent assessment.

7.9.1.4 Server rooms and other related security zones where ICT equipment are kept shall be secured with adequate security measures and strict access control shall be enforced and monitored.

7.9.1.5 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 or peripherals of the institution shall be restricted unless explicitly authorized.

7.9.1.6 System hardware, operating an application software, the network and communication systems of the institution shall be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

7.9.1.7 All employees shall make use of ICT systems of the institution in an acceptable manner and for business purposes only. All employees must comply with the ICT Security Directives in this regard at all times.

7.9.1.8 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 and should be changed on a monthly period as per ICT Passwords Policy in place.

7.9.1.9 To ensure the on-going availability of critical services, the institution shall develop ICT continuity plans as part of the overall Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP).

7.10 Internet

7.10.1 The Assistant Manager ICT 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 minimum, a

configured firewall. ICT unit assisted by the Human Resource Management Unit 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.

7.10.2 The Assistant Manager ICT of the Municipality 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 safeguard, to reduce the risk of Information Security Breaches and incidents.

7.10.3 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 codes.

7.11 Use of Laptop Computers

7.11.1 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.

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

7.11.3 Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop computers at all times, in line with the protection measures prescribed in the ICT Policy.

{negligent loss or damage to laptops or computers should be followed by consequence steps taken}

See Security Directive on Information Security/Categorization of information and information classification.

7.12 Communication Security

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

7.12.2 All sensitive electronic communication by employees, contractors and consultants of the Municipality must be encrypted in accordance with the South African Communication 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.

7.12.3 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 TOP SECRET clearance who successfully completed the SACSA Course)

7.13 Technical Surveillance Counter Measures (TSCM)

7.13.1 All offices, meetings, 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) shall be conducted by the National State Security Agency to ensure that these areas are kept sterile and secure.

7.13.2 The Security Manager of the Municipality shall ensure that areas that are utilized for discussion of sensitive nature as well as offices or rooms that house electronic communication equipment, are physically secured in accordance with the standards laid down by the National State Security Agency in order to support the sterility of the environment after TSCM examination, before any request for a TSCM is submitted.

7.13.3 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.

7.14 Business Continuity Planning (BCP)

7.14.1 Both the Security Manager, ISO and Assistant Manager ICT should update and review 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 employees, contractors, consultants and visitors.

7.14.2 The BCP shall be periodically tested to ensure that the management and employees of the Municipality understand how it is to be executed.

See Security Directive on Physical Security.

7.14.3 All employees of the institution shall be made aware and trained on the content of the Business Continuity Plan to ensure understanding of their own respective roles in terms thereof.

7.14.4 The Business Continuity Plan shall be kept up to date and re-tested periodically by the Security Manager, ISO, Chief Risk Officer and ICT Manager.

8. Specific Responsibilities

8.1 Head of Institution

8.1.1 The Municipal Manager bears the overall responsibility for implementing and enforcing the security program of the institution. Towards the execution of this responsibility, the Executive Director: Corporate 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.

8.2 Security Manager

8.2.1 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 (coordinating, planning, implementation, controlling, evaluation, monitoring, 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 specific and detailed security directives of the institution in conjunction with the security committee.
- Review the Security Policy and Security Plan at a regular interval.
- Conduct the security Threat and Risk Analysis of the institution with the assistance of the security committee.
- Advice management on the security implications of the management decisions.
- Implement a security awareness program.
- Conduct internal compliance audits and inspections at the Municipality at regular intervals.

- Establish a good working relationship with both the SAPS and SSA and liaise with these institutions on a regular basis.
- As mentioned in paragraph 8.2.1 Security Manager should have delegated signing powers as per Municipal Manager's and Executive Director: Corporate Service's discretion.

8.3 Security Committee

8.3.1 The Security Committee shall consist of Senior Managers of the Municipality representing all the main business units of the Municipality.

8.3.2 Participation in the activities of the Security Committee by the appointed representatives of the business units in the Municipality shall be compulsory. [failure to adhere must receive the attention of the Accouncting Officer].

8.3.3 The Security Committee responsibilities shall assist the Security Manager in the execution of all security related responsibilities of the Municipality. The Security Committee shall assist in:

- Completing tasks such as assisting in the drafting and reviewing of the security Policy and Plan.
- Conducting Threat and Risk Assessment exercise.
- Conducting security audits.
- Assist in drafting of the Business Continuity Plan and;
- Assisting with security awareness and training.

8.4 Managers

8.4.1 All managers of the Municipality shall ensure that all their subordinates comply with this policy and the Security Directives as contained in the security plan of the Municipality.

8.4.2 All managers must ensure that appropriate measures are implemented and steps are taken immediately to rectify any non-compliance issue that may come to their attention. This includes the taking of disciplinary action against employees if warranted [on receiving a directive from the secutity manager.

8.5 Employees, Contractors, Consultants and other Service Providers

8.5.1 All employees, contractors, consultants and other service providers of Victor Khanye Local Municipality shall know what their security responsibilities are, and 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.

8.5.2 Some of their responsibilities include amongst others:

See Security Directive on Vetting/Personnel Suitability Checks.

- Identifying possible security weaknesses and threats and reporting to the Security Manager.
- Reporting any form of and or suspected security breach conducted either internally or externally.
- Attend security awareness programs and training.
- Participate in security emergency drills.
- Comply with the Policy and Security Plan of the Municipality.

9. Enforcement, Exception and other Considerations

9.1 Enforcement

9.1.1 The Municipality Manager, Executive Dircetor Corporate Services and the appointed Security Manager are accountable for the enforcement of the Security Policy.

9.1.2 All employees of the Municipality are required to fully comply with the policy and its associated Security Directives as contained in the Security Plan. Non-Compliance with any prescript shall be addressed in terms of the Disciplinary Code/Regulations of the Municipality.

9.1.3 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 individuals, institutions/companies. The consequences of any transgression/deviation or non-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.

9.2 Exceptions

9.2.1 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 the people.
- During an unavoidable emergency circumstances such as a natural disaster.
- On a written permission of the Security Manager and the 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.

9.3 Other Considerations

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

- Occupational Health and Safety issues of Victor Khanye Local Municipality.
- Disaster Management of Victor Khanye Local Municipality.
- 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.
- Environmental issues as prescribed and regulated in relevant legislation such as when implementing physical security measures that may impact on the environment.

10. Communication Policy

10.1 The Security Manager of Victor Khanye Local 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.

10.2 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 Municipality.

11. Parking Policy

11.1 The overall responsibility for the administration and interpretation of the Parking policy lies with the corporate Services {HRM} Facilities Management Directorate.

11.2 The purpose thereof is to establish clearly the principles by which parking administration and allocations are made at all Victor

Khanye Local Municipality Offices and Buildings.

12. Cash Points

12.1 Notwithstanding provisions made in the banking policy of the Municipality, all cashiers must ensure that a maximum of a R1000.00 is not exceeded in their till. All excess monies to be dropped into the drop safe.

12.2 Security officers must patrol cash points on a regular base and must sign on the occurrence book.

12.3 All incidents and suspicions must be reported immediately to the Security Manager

13. Search of Vehicles and Persons

13.1 All vehicles intending to gain access into the Municipal premises will be subjected to a search. The vehicles will include those belonging to the public and employees however such will exclude Councillors

13.2 Any person who refuses to be searched may not be allowed into the Municipal premises.

13.3 All pedestrians must be subjected to a scan at all entry points

See ICT Policy to be compiled.

14. Review and Updates Process

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

15. Implementation

15.1 The Security Manager of Victor Khanye Local Municipality must manage the implementation process of this policy and its associate Security Directives by means of an action plan.

15.2 Implementation of the policy and its associated directives is the responsibility of each and every individual this policy is applicable.

16. Monitoring

16.1 The Security Manager, with the assistance of the security component and 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 inspections on a regular basis.

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

17. Disciplinary Actions

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

- Re-training
- Verbal and written warning
- Termination of contract in the case of contractors or consultants delivering a service to the Municipality.
- Dismissal
- Suspension
- Loss of Institution information and asset resources access privileges.

17.2 Any disciplinary action taken in terms of non-compliance with this policy and its associated security directives will be in accordance with the disciplinary code or directives [including relevant legislation] of the Victor Khanye Local Municipality.

18. Supporting Documents

18.1 Security Plan containing the following:

- Security Component Organizational Structure
- Security Component Officers Positions.
- Specific responsibilities of key stakeholders
- Security Directive: Reporting of Security Breaches
- Security Directive: Security Breach response procedures
- Security Directive: Information Security: General Responsibilities
- Security Directive: Classification System
- Security Directive: Security Screening/Vetting
- Security Directive: Physical Security
- Security Directive: Access Control
- Security Directive: ICT Security
- Security Directive: Secure Discussion Areas
- Security Directive: Threat and Risk Assessment (TRA)
- Security Directive: Security Audits and Inspections
- ICT Security Policy
- Business Continuity Plan (BCP)
- Occupational Health and Safety (OHS) Policy
- Disciplinary Code
- Supply Chain Management Policy
- Contract Management Policy

19. Approval of the Policy

Document Name Security Policy and Procedures

Signature _____ _____

Municipal Manager Date

Adopted by Mayoral _____ _____

Committee Chairperson Date

Approved by Council _____ _____

Resolution Date

Effective Date _____

Next revision Date One year from the effective date