67 Church Street, Mt Ayliff, 4735
Tel: +27 (0)39 254 6000
Fax: +27 (0) 39 255 0167
Web : www.umzimvubu.gov.za

813 Main Street , Mount Frere
P/ Bag 9020, M t Frere , 5090
Tel: +27 (0)39 255 8500 /166
Fax: +27 (0) 39 255 0167

UMZIMVUBU
LOCAL MUNICIPALITY

UMZIMVUBU LOCAL MUNICIPALITY

UMZIMVUBU MUNICIPALITY SECURITY SERVICES POLICY

UMZIMVUBU SECURITY SERVICES POLICY
DATE:
AGENDA: COUNCIL MEETING:

CITIZEN & COMMUNITY SERVICES DEPARTMENT

UMZIMVUBU MUNICIPALITY SECURITY SERVICES POLICY

1. PURPOSE

The purpose for the policy is to support the National Interest and the Umzimvubu Local Municipality business objectives by protecting employees, information, asset and assuring the continued delivery of services to South African citizens and residents. The Municipality Management must put appropriate measures to protect the Municipality assets, Information and life of its staff and visitors against any form of threat.

2. BACKGROUND

Attached hereto is the Security Policy for Security Personnel.

3. LEGAL IMPLICATION

It is compliance in terms of the governing legislation that governs us.

4. CURRENT POLICY

None

5. OTHER PARTIES CONSULTIES

Management and Senior Management

6. DELEGATION

Council

7. RECOMMENDATIONS

1. That Council adopt the Security Policy for Security Personnel working for Umzimvubu Local Municipality.

2. That the Policy become effective after council adoption. (FOR RECOMMENDATION TO COUNCIL).

SECURITY POLICY FOR UMZIMVUBU LOCAL MUNICIPALITY

1. STATEMENT OF PURPOSE

1.1 The Umzimvubu Local Municipality depends on its personnel, information and assets to deliver services that ensure the health, safety, security and economic well-being of South African citizens. It must therefore manage these resources with due diligence and take appropriate measures to protect them.

1.2 Threats that can cause harm to Umzimvubu Local 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 result of changes in the international environment.

1.3 The Security Policy of Umzimvubu 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 employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of services. Since the Umzimvubu Local 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.

1.4 The main objective of this policy therefore is to support the national interest and the Umzimvubu Local Municipality business objectives by protecting employees, information and assets and assuring the continued delivery of services to South African citizens.

1.5 This policy complements other Umzimvubu Local Municipality policies.

2. SCOPE

2.1 This policy applies to the following individuals and entities:

- The Mayor and Councillors
- The Municipal Manger and other Managers
- all employees of Umzimvubu Local Municipality,

  all contractors and consultants delivering a service to Umzimvubu

Local Municipality, including their employees who may interact with Umzimvubu Local Municipality;

- temporary employees of Umzimvubu Local Municipality;
- all information assets of Umzimvubu Local Municipality;
- all intellectual property of Umzimvubu Local Municipality;
- all fixed property that is owned or leased by Umzimvubu Local Municipality;
- all moveable property that is owned or leased by Umzimvubu Local Municipality.

2.2 The policy further covers the following seven elements of the Security program of Umzimvubu Local Municipality:

- Security organization
- Security information
- Information security
- Physical security
- Personal security
- Information and Communication Technology (ICT) security
- Business continuity Planning (BCP)

3. LEGISLATIVE AND REGULATORY REQUIREMENTS

3.1 This policy is informed by and complies with applicable national Legislation, national security policies and national security standards. A list of applicable regulatory document in this regard has been attached at Annex A.

4. POLICY STATEMENT

4.1 General

- Employees of Umzimvubu Local Municipality must be protected against identified threats and according to baseline security requirements and continuous security risk management.

- Information and assets of Umzimvubu Local Municipality protected according to baseline security requirements and continuous security risk management.
- Continued delivery of services of Umzimvubu Local Municipality must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

4.2 **Compliance requirements**

4.2.1 All individuals mentioned in par.2 above must comply with the baseline requirements of this policy and its associated Security Directives. These requirements are/shall be based on integrated security **Threat and Risk Assessments** (TRA's) to the national interest as well as employees, information and assets of Umzimvubu Local Municipality. The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.

4.2.2 Security threat and risk assessments involve:

- Establishing the scope of the assessment and identifying the information, employees and assets to be protected.
- Determining the threats to information, employees and assets of Umzimvubu Local Municipality 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.

4.2.3 **Staff accountability and acceptable use of assets**

4.2.3.1 The Accounting Officer/ Municipal Manager of Umzimvubu Local Municipality shall ensure that information and assets of Umzimvubu Local Municipality are used in accordance

With procedures as stipulated in the Security Directives as contained in the Security Plan of Umzimvubu Local Municipality?

4.2.3.2 All employees of Umzimvubu Local Municipality shall be accountable for the proper utilization and protection of such information and assets. Employee/s that misuse or abuse assets of Umzimvubu Local Municipality shall be accountable therefore and disciplinary action shall be taken against any such employee/s.

4.3 **Specific baseline requirements**

4.3.1 **Security organization**

4.3.1.1 The Accounting Officer/Municipal Manager of Umzimvubu Local Municipality will appoint a Security Manager (SM) to establish and direct a security program that ensures coordination of all policy functions and implementation of policy requirements.

4.3.1.2 Given the importance of this role, a SM with sufficient security experience and training who is strategically positioned within the Umzimvubu Local Municipality so as to provide institution-wide strategic advice and guidance to senior management, will be appointed.

4.3.1.3 The Accounting Officer/Municipal Manager will ensure that the SM has an effective support structure (security component) to fulfil the functions referred to in par. 4.3.2 below.

4.3.1.4 Individuals that will be appointed in the support structure of the SM will all be security professionals with sufficient security experience and training to effectively cope with their respective job functions.

4.3.2 **Security administration**

4.3.2.1 The functions referred to in par. 4.3.1 above include:

- general security administration (training and awareness, security risk management, security audits, sharing of information and assets;
- setting of access limitations;
- administration of security screening;
- implementing 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 and facilitating security breach reporting and investigations.

4.3.2.2 **Security incident/breaches reporting process**

4.3.2.2.1 Whenever an employee of Umzimvubu Local Municipality becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidentally or intentionally), he/she shall report that to the SM of Umzimvubu Local Municipality.

4.3.2.2.2 The Accounting Officer/Municipal Manager of Umzimvubu Local Municipality shall report to the appropriate authority all cases or suspected cases of security breaches, for investigation.

43.2.2.3 The SM of Umzimvubu Local Municipality shall ensure that all employees are informed about the procedure for reporting security breaches.

4.3.2.3 **Security incident/breaches response process**

4.3.2.3.1 The SM shall develop and implement security breach response mechanisms for Umzimvubu Local Municipality in order to address all security breaches/alleged breaches which are reported.

4.3.2.3.2 The SM shall ensure that the Accounting Officer/Municipal Manager of Umzimvubu Local Municipality is advised of such incidents as soon as possible.

4.3.2.3.3 It shall be the responsibility of the National Intelligence Structures (e.g. the SSA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendation to Umzimvubu Local Municipality.

4.3.2.3.4 Access privileges to classified information, assets and/or to premises may be suspended by the Accounting Officer/Municipal Manager of Umzimvubu Local Municipality until administrative, disciplinary and/or criminal processes have been concluded, following from investigations into security breaches or alleged security breaches.

4.3.2.3.5 The end result of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the Accounting/ Municipal Manager of Umzimvubu Local Municipal 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.

4.3.3 **Information security**

4.3.3.1 **Categorization of information and information classification system**

4.3.3.2 The SM must ensure that a comprehensive information classification system is developed for an implementation in Umzimvubu Local Municipality. All sensitive information produced or processed by Umzimvubu Local Municipality must be identified, categorized and classified according to the origin of

its source and contents and according to its sensitivity to loss or disclosure.

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

- State Secret
- Trade Secret and
- Personal Information

and subsequently classified according to its level of sensitivity by using one of the recognised levels of classification:

- Confidential
- Secret, and
- Top Secret

4.3.3.4 Employees of Umzimvubu Local Municipality who generate 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.

4.3.3.5 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.

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

- intrinsic secrecy approach;
- need - to - know;
- level of security Clearance.

4.3.4 Physical Security

4.3.4.1 Physical security involves the proper layout and design of facilities of Umzimvubu Local Municipality and the use of physical security measures to delay and prevent unauthorized access to

assets of Umzimvubu Local Municipality. 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.

4.3.41 Physical security measures must be developed, implemented and maintained in order to ensure that the entire Umzimvubu Local 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 SM.

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

- select, design and modify facilities in order to facilitate the effective control of access thereto;
- demarcate restricted access 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 document;
- incorporate related costs in funding requirements for the implementation of the above.

4.3.4.4 Umzimvubu Local 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.

4.3.4.5 All employees are required to comply with access control procedures of Umzimvubu Local Municipality at all times. This includes the producing of ID Cards upon entering any sites of

Umzimvubu Local Municipality, the display thereof whilst on the premises and the escorting of official visitors.

4.3.5 **Personnel Security**

4.3.5.1 **Security Vetting**

4.3.5.1.1 **All** employees, contractors and consultants of Umzimvubu Local 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 vetting investigations conducted by the State Security Agency(SSA) in order to be granted a security clearance at the appropriate level.

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

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

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

4.3.5.1.5 A security clearance will be valid for a period of ten years in respect of the 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 Accounting Officer/ Municipal Manager of Umzimvubu Local Municipality, based on information which impact negatively on an individual's security competence.

4.3.5.1.6 Security clearances in respect of all individuals who have terminated their services with Umzimvubu Local Municipality, shall immediately be withdrawn.

4.3.5.2 **Polygraph examination**

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

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

4.3.5..4 **Transferability of security clearances**

4.3.5.4.1 A security clearance issued in respect of an official from other government institutions shall not be automatically transferable to the Umzimvubu Local Municipality. The responsibility for deciding whether the official should be re-screened rests with the Accounting Officer/ Municipal Manager of Umzimvubu Local Municipality.

4.3.5.4 Security Awareness and Training

4.3.5.4.1 A security training and awareness program must be developed by the SM and implemented to effectively ensure that all personnel and service providers of Umzimvubu Local Municipality remain security conscious.

4.3.5.4.2 All employees shall be subjected to the security awareness and training programs and must certify that the contents of the programs has been understood and will be complied with. The program must cover/covers training with regard to specific security responsibilities and sensitize employees and relevant

contractors and consultants about the security policy and security measures of Umzimvubu Local Municipality and the need to protect sensitive information against disclosure, loss and destruction.

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

4.3.5.4.4 Regular surveys and walkthrough inspections shall be conducted by the SM and members of the security component to monitor the effectiveness of the security training and awareness program.

4.3.6 **Information and Communication Technology (ICT) Security**

4.3.6.1. IT Security

4.3.6.1.1 A secure network shall be established for Umzimvubu Local 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.

4.3.6.1.2 To prevent the compromise of IT systems, Umzimvubu Local Municipality shall implement baseline security controls and any additional control 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.

4.3.6.1.3 To ensure policy compliance, the IT Manager of Umzimvubu Local 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;
- Periodic request assistance, review and audits from the State Security Agency (SSA) - in order to get an independent assessment.

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

4.3.6.1.5 Access to the resources on the network of Umzimvubu Local Municipality shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of Umzimvubu Local Municipality shall be restricted unless explicitly authorized.

4.3.6.1.6 Systems hardware, operating and application software, the network and communication systems of Umzimvubu Local Municipality shall all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

4.3.6.1.7 All employees shall make use of IT systems of Umzimvubu Local Municipality in an acceptable manner and for business purpose only. All employees shall comply with the IT Security Directives in this regard at all times.

4.3.6.1.8 The selection of passwords, their use and management as a primary means to control access to systems is strictly adhere to back up practice guidelines as reflected in the IT Security Directives. In particular, passwords shall not be shared with any other person for any reason.

4.3.6.1.9 To ensure the ongoing availability of critical services, Umzimvubu Local Municipality shall develop IT continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.

4.3.6.2 **Internet access**

4.3.6.2.1 The IT Manager of Umzimvubu Local Municipality, having the overall responsibility for setting up Internet access for Umzimvubu Local Municipality, shall ensure that the network of Umzimvubu Local Municipality is safeguarded from malicious external intrusion by developing, 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 Internet.

4.3.6.2.2 The IT Manager of Umzimvubu Local Municipality shall be responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguard, to reduce the risk of information Security breaches and incidents.

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

4.3.6.3 **Use of laptop computers**

4.3.6.3.1 Usage of laptop computers by employees of Umzimvubu Local 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.

4.3.6.3.2 The information stored on a laptop/computer of Umzimvubu Local Municipality shall be suitably protected at all times, in line with the protection measures prescribed in the IT Security Directive.

4.3.6.3.3 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 IT Security Directive.

4.3.6.4 **Communication security**

4.3.6.4.1 The application of appropriate security measures shall be instituted in order to protect all sensitive information and confidential communication of Umzimvubu Local Municipality in all its forms and at all times.

4.3.6.4.2 **All** sensitive electronic communications by employees, contractors or employees of Umzimvubu Local Municipality must be encrypted in accordance with Communication Security (COMSEC) standards and the Communication Security Directive of Umzimvubu Local Municipality.

4.3.6.4.3 Access to communication security equipment of Umzimvubu Local Municipality and handling of information transmitted and /or received by such equipment, shall be restricted to authorized personnel only (personnel with Top Security Clearance who successfully completed the COMSEC Course).

4.3.6.5 Technical surveillance counter measures (TSCM)

4.3.6.5.1 All offices, meeting, conference and boardroom venues of Umzimvubu Local 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 and sweeping will be conducted by the SSA to ensure that these areas are kept sterile and secure.

4.3.6.5.2 The SM of Umzimvubu Local Municipality shall ensure that areas that are utilized for discussions of a sensitive nature as well as

offices or rooms that house electronic communication equipment, are physically secured in accordance with standards laid down by the SSA in order to support the sterility of the environment after TSCM examination, before any request for TSCM examination is submitted.

4.3.6.5.3 No unauthorized electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of Umzimvubu Local Municipality is discussed. Authorization must be obtained from the SM.

4.3.7 **Business Continuity Planning (BCP)**

4.3.7.1 The SM of Umzimvubu Local Municipality 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 employees, contractors, consultants and visitors.

4.3.7.2 The business continuity plan (BCP) shall be periodically tested to ensure that the management and employees of Umzimvubu Local Municipality understand how it is to be executed.

4.3.7.3 All employees of Umzimvubu Local Municipality shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.

4.3.7.4 The Business Continuity Plan shall be kept up to date and re-tested periodically by the SM.

5. SPECIFIC RESPONSIBILITIES 5.1

Head of institution

5.1.1 The Accounting Officer/ Municipal Manager of Umzimvubu Local Municipality bears the overall responsibility for implementing and

Enforcing the security program of Umzimvubu Local Municipality. Towards the execution of this responsibility, the Accounting Officer/ Municipal Manager shall:

- establish the post of the SM and appoint a well-trained and competent security official in the post;
- establish a security committee for the institution and ensure the participation of all senior management members of all the core business functions of Umzimvubu Local Municipality in the activities of the committee;
- approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

5.2 **Security Manager**

5.2.1 The delegated security responsibility lies with the SM of Umzimvubu Local Municipality who will be responsible for the execution of the entire security function and program within Umzimvubu Local Municipality (coordination, planning, implementing, controlling, etc). Towards execution his/her responsibilities, the SM shall, amongst others:

- chair the security committee of Umzimvubu Local Municipality;
- draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of Umzimvubu Local Municipality in conjunction with the security committee;
- review the Security Policy and Security Plan at regular intervals;
- conduct a security TRA of Umzimvubu Local Municipality with the assistance of the security committee;
- advise management on the security implications of management decisions;
- implement security awareness program
- conduct internal compliance audits and inspections at Umzimvubu Local Municipality at regular intervals'
- Establish a good working relationship with both SSA and SAPS and liaise with these institutions on a regular basis.

5.3.1 The Security Committee referred to in par. 5.1.1 above shall consist of senior managers of Umzimvubu Local Municipality representing all the main business units of Umzimvubu Local Municipality.

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

5.3.3 The Security Committee of the Umzimvubu Local Municipality shall be responsible for, amongst others:

- assisting the SM in the execution of all security related responsibilities at Umzimvubu Local 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.

5.4 **Line Management**

5.4.1 All managers of Umzimvubu Local Municipality shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of Umzimvubu Local Municipality at all times.

5.4.2 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.

5.5 **Employees, Consultants, Contractors and other Service Providers**

5.5.1 Every employee, consultants, contractor and other service providers of Umzimvubu Local 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 Umzimvubu Local Municipality at all times.

6. AUDIENCE

6.1 This policy is applicable to all members of the management, politicians, employees, consultants, contractors and any other service providers of Umzimvubu Local Municipality. It is further applicable to all visitors and members of the public visiting premises of or may officially interact with Umzimvubu Local Municipality.

7. ENFORCEMENT

7.1 The Accounting Officer/ Municipal Manager of Umzimvubu Local Municipality and the appointed SM are accountable for the enforcement of this policy.

7.2 All employees of Umzimvubu Local Municipality are required to fully comply with this policy and its associated Security Directives as contained in the Security Plan. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code/ Regulations of Umzimvubu Local Municipality.

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

8. EXCEPTIONS

8.1 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 Accounting Officer/ Municipal Manager of Umzimvubu Local Municipality (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. OTHER CONSIDERATIONS

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

9.1.1 All existing Umzimvubu Municipal Policies.

9.1.2 Occupational Health and Safety issues in the Umzimvubu Local Municipality.

9.1.3 Disaster management at Umzimvubu Local Municipality.

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

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

10. COMMUNICATING THE POLICY

10.1 The SM of Umzimvubu 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 Umzimvubu Local Municipality. The SM will further ensure that all security policy and directive prescriptions are enforced and complied with.

10.2 The SM must ensure that a comprehensive security awareness program is developed and implemented within Umzimvubu Local Municipality to facilitate the above said communication. Communication of the 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 Umzimvubu Local Municipality.

11. REVIEW AND UPDATE PROCESS

11.1 The SM, assisted by the Security Committee of Umzimvubu Local 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.

12. IMPLEMENTION

12.1 The SM of Umzimvubu Local 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 Umzimvubu Local Municipality.

12.2 Implementation of the policy and its associated Security Directives is the responsibility of each and every individual this policy is applicable too (see par.2.1 above)

13. MONITORING OF COMPLIANCE

13.1 The SM, with the assistance of the security component and security committee of Umzimvubu Local Municipality must ensure compliance with this policy and its associated Security Directives by means of conducting internal security audits and inspections on as frequent basis.

13.2 The findings of said audits and inspections shall be reported to the Accounting Officer/ Municipal Manager.

14. DISCIPLINARY ACTION

14.1 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 warning;
- termination of contracts in the case of contractors or consultants delivering a service to Umzimvubu Local Municipality;
- dismissal;
- suspension;
- Loss of Umzimvubu Local Municipality information and assets resources access privileges.

14.2 Any disciplinary action taken in terms of non-compliance with this policy and its associated directives will be in accordance with the disciplinary code/directive of Umzimvubu Local Municipality.

ANNEX A APPLICABLE LEGISLATION AND OTHER REGULATORY FRAMEWORK DOCUMENTS

Applicable legislation

- Constitution of the Republic of South Africa, 1996(Act 106 Of 1996)
- Protection of Information Act, 1982(Act no 84 of 1982)
- Promotion of access to Information Act,2000 (Act no 2 of 2000)
- Promotion of Administrative Justice Act, 2000 (Act 3 Of 2000)
- Copyright Act, 1978(Act no 98 of 1978)
- National Archives of South Africa Act, 1996(Act no 43 of 1996) and regulations
- Public Service Act, 1994(Act no 103 of 1994) and regulations

- Occupational Health and Safety Act,1993(Act no 85 of 1993)
- Criminal Procedure Act, 1977(Act 51 of 1977), as amended.
- Private Security Industry Regulations Act, 2001(Act 56 Of 2001)
- Control of Access to Public Premises and Vehicles Act,1958(Act 53 of 1985)
- National Key Points Act, 1980(Act 102 of 1980)
- Trespass Act, 1959(Act 6 of 1959)
- Electronic Communication and Transaction Act,2002(Act 25 of 2002)
- Electronic Communications Security (Pty) Ltd Act,20029Act 68 of 2002)
- State Information Technology Agency Act,1998(Act88 of 1998)
- Regulation of Interception of Communications and Provision of Communication- Related Information Act, 2002(Act 70 of 2002)
- General Intelligence Law Amendment Act,2000 (Act 66 Of 2000)
- Intelligence Service Act,2002(Act 65 of 2002) and regulations
- National Strategic Intelligence Act,1994(Act 39 of 1994)
- Intelligence Service Control Act,1994(Act 40 of 1994)
- Labour Relations Act, 1995(Act 66 of 1995)
- Employment Equity Act,1998 (Act 55 of 1998)
- Occupational Health and Safety Act,1993(Act 83 of 1993)
- Fire-arms Control Act,2000(Act 60 of 2000(Act 60 of 2000) and regulations
- Non-Proliferation of Weapons of Mass Destruction Act,1993(Act 87 of 1993)
- Protection of Constitutional Democracy Against Terrorism and Related Activities Act,2004(Act33 of 2004)
- National Building Regulations and Building Standards Act,1977(Act 103 of 1977)
- Protected Disclosure Act, 2000(Act 26 of 20000
- Intimidation Act,1982(Act 26 Of 2000)
- Prevention Combating of Corrupt Activities Act, 2004(Act 12 of 2004)
- Municipal Finance Management Act 2003(Section

Other regulatory framework documents

- Minimum Information Security Standards (MISS) Second Edition March 1998
- White paper on Intelligence (1995)
- SACSA/090/1(4) Communication Security in the RSA
- SSA Guidance Documents: ICT Policy and Standards: Part1&2
- ISO 17799
- National Building Regulations

ANNEX B GLOSSARY AND DEFINITIONS

- "accreditation" means the official authorisation by management for the operation of an Information Technology (IT) system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations;
- "assets" means material and immaterial property of an institution. Assets include but are not limited to information in all forms and stored on any media, networks or systems, or material, real property, financial recourses, employee trust, public confidence and international reputation;
- "availability" means the condition of being usable on demand to support operations, programmes and services;
- "business continuity planning" includes the development of -plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical services and assets;
- "candidate" means applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor;

- "certification" means the issuing of a certificate certifying that a comprehensive evaluation of technical and non-technical security features of an information and Communication

Technology system (hereinafter referred to as an "ICT" system) and its related safeguards has been undertaken and that it was established that its design and implementation meets a specific set of security requirements;

- "comsec" means the organ of state known as Electronic Communications Security (Pty) Ltd, which was established in terms of section 2 of the Electronic Communications Security Act,2002 (Act no.68 of 2002) and, until such time as COMSEC becomes operational , the South African Communication Security Agency;
- "critical services" means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the institution;
- "document" means-

any note or writing, whether produced by hand or by printing, typewriting or any other similar process, in either tangible or electronic format; any copy, plan, picture, sketch or photographic or other representation of any place or article;

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

- "information security includes, but is not limited to, -document security;

physical security measures for the protection of information;

information and communication technology security; personnel security;

business continuity planning;
contingency planning;
security screening;
technical surveillance counter measures;
dealing with information security breaches;
security investigations; and
administration and organization of the security function at organs of state;

- "national intelligence structures" means the National Intelligence Structures as defined in section 1 of the National Strategic Act, Act 39 of 1994;

- "reliability check" means an investigation into the criminal record, credit record and past performance of an individual or private organ of state to determine his/ her or its reliability;
- "risk" means the likelihood of a threat materialising by exploitation of a vulnerability;
- "screening investigator" means a staff member of a National Intelligence Structure designated by the head of the relevant National Intelligence Structure to conduct security clearance investigations;
- "security breach" means the negligent or intentional transgression of or failure to comply with security measures
- "security clearance" means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the need to know';
- "site access clearance" means clearance required for access to installations critical to the national interest;
- "technical surveillance countermeasures" (TSCM) means the process involved in the detection, localisation, identification and neutralisation of technical surveillance of an individual, an organ of state, facility or vehicle;
- "technical/electronic surveillance" means the interception or monitoring of sensitive or proprietary information or activities (also referred to as "bugging");
- "threat" means any potential event or act, deliberate or accidental, that could cause injury to persons, compromise the integrity of information or could cause the loss or damage of assets;
    - "threats and risk assessment (TRA)" means, within the context of security risk management, the process through which it is determine when to avoid, reduce and accept risk, as well as how to diminish the potential impact of a threatening event;
    - "vulnerability" means a deficiency related to security that could permit a threat to materialise.

ANNEX C SUPPORTING DOCUMENTS

- Security Plan containing the following: - Operating Procedure for Security Personnel.

AUTHENTICATION

The amendments of the policy and or the new policy was adopted by the council on the

……..

As per Council Resolution number:

Signed off

_____	_____
Mr. G.P.T. Nota	**Cllr. N.F. Ngonyolo**
Municipal Manager	**Speaker of the Council**