Tirisano Motheo Tswelopele
FETAKGOMO LOCAL MUNICIPALITY
Provisional

FETAKGOMO – GREATER TUBATSE
LOCAL MUNICIPALITY

NTSEE KGOPU
The GTM
GREATER TUBATSE
MUNICIPALITY
South Africa's first democratic platinum city

SECURITY POLICY

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 **Fetakgomo - Greater Tubatse 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

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 the **Fetakgomo - Greater Tubatse 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.

Fetakgomo - Greater Tubatse 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 the Fetakgomo - Greater Tubatse 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 the ***Fetakgomo - Greater Tubatse 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 the 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 all employees.

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

This policy complements other policies of the Municipality (e.g. sexual harassment, occupational health and safety, information management, asset control, 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:

- The Mayor, the Speaker, Chief Whip, and all other Councilors
- The Municipal Manager, and all section 57 Managers
- All employees of the Fetakgomo - Greater Tubatse 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 all applicable National legislation, National security policies and national security standards. Lists 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)
- Fire-arms Control Act, 2000 (Act 60 of 2000)
- Hazardous Substances Act, 1973 (Act 15 of 1973)
- 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)
- 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 Mayor, Speaker, Chief Whip, Exco Members, Councilors, Accounting Officer, all employees and visitors to the ***Fetakgomo - Greater Tubatse Municipality*** against identified threats according to baseline security requirements and continuous risk management.

- To secure the information and assets of the Fetakgomo - Greater Tubatse Municipality against identified threats according to baseline security requirements and continuous risk management.

- To ensure continued delivery of services of the Fetakgomo - Greater Tubatse 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 the *Fetakgomo - Greater Tubatse 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 the 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 the Municipality.

5.3.2 All employees of the 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 the security 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 and Risk Management unit of the institution by utilizing the formal reporting procedure prescribed by the Security Breach Directive of the institution.

5.5.2 The Security and Risk Management unit 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 and Risk Management unit 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 and Risk Management unit 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 and Risk Management unit shall ensure that the Accounting Officer is informed and advised as soon as possible.

5.6.3 It shall be the responsibility of the National Intelligence structures (e.g. SASSA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendations to the municipality.

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.

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 and Risk management unit must ensure that a comprehensive information classification system is developed and implemented in the municipality. 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.

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 the Fetakgomo – Greater Tubatse Municipality and the use of physical security measures to delay and prevent unauthorized access to assets of the 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.

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 and Risk Management Unit.

5.8.3 The 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 Fetakgomo- Greater Tubatse 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 the Fetakgomo- Greater Tubatse 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 State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

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 Municipality. The responsibility for deciding whether the official should be rescreened 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 and Risk Management unit 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 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 and Risk Management Unit 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.

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 State Security Agency (SSA) 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 municipality 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 Manager 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 Manager 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, in line 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 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 State Security Agency (SSA) to ensure that these areas are kept sterile and secure.

5.17.2 The Security and Risk 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 State Security Agency (SSA) 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 municipality is discussed. Authorization must be obtained from the Security and Risk Management unit.

5.18 Business Continuity Planning (BCP)

5.18.1 Both the Security Risk Management and IT Managers 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.

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 and Risk Management and IT Manager.

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 municipality, towards the execution of this responsibility, the Municipal Manager shall:

- Establish the post of the Security and Risk 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.

6.2 Security and Risk Manager

6.2.1 The delegated security responsibilities lies with the Security and Risk Management Unit 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/Officer 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 SSA and liaise with these institutions on a regular basis.

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

8.1Every employee, Contractor, Consultant and other Service Providers of the Greater Tubatse 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 the Fetakgomo - Greater Tubatse Municipality. It is further applicable to all visitors and members of the public visiting premises of municipality or may officially interact with the institution.

10. ENFORCEMENT

10.1 The Municipal Manager, all Directors 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 its associated Security Directives as contained in the Security Plan. Noncompliance 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 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.

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 noncompliance 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

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

12.1 Occupational Health and Safety issues of the Fetakgomo- Greater Tubatse Municipality.

12.2 Disaster Management of the Fetakgomo - Greater Tubatse Municipality.

12.3 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.

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

13. COMMUNICATION OF THE POLICY

13.1 The appointed Security Manager of the 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 appointed Security Manager will further ensure that all security policy and directive prescription are enforced and complied with.

13.2 The appointed 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. REVIEW AND UPDATE PROCESS

14.1 The appointed Security Manager, assisted by the Security Committee of the Municipality, must ensure that this policy and its associated Security Directives is reviewed and updated as and when required. Amendments shall be made to the policy and directives as the need arise.

15. IMPLEMENTATION

15.1 The Security Manager of the Municipality must manage the implementation process of this policy and it's 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).

15.2 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).

16. MONITORING

16.1 The Security and Risk Manager, with the assistance of the security and risk 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.

16.2 The findings 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 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.

17.2 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.

18. DEFINITION OF TERMS

18.1 Access Control

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

18.2 Classification

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

18.3 Contingency Planning

8.3.1 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 practice thereof, in order to identify and rectify gaps in the plan, and to familiarise personnel and coordinators with the plan.

18.4 Computer Security

18.4.1 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.

18.4.2 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.

18.5 Communication Security

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

18.6 Declaration of Secrecy

18.6.1 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.

18.7 Delegation

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

18.8 Document

18.8.1 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.

18.9 Document Security

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

18.10 Employees

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

- Permanent staff;
- Temporary staff; and
- Contract staff.

18.11 Information Security

18.11.1 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.

18.12 Personnel security

18.12.1 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.

18.13 Physical security

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

18.14 Premises

18.14.1For the purpose of this policy, premises shall refer to any building, structure, hall, room, office, land which is the property of, or is occupied by, or is under the control of Greater Tubatse Municipality and to which a member of the public has a right of access.

18.15 Screening Institution

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

18.16 Security

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

18.17 Security audit

18.17.1 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.

18.18 Security clearance

18.18.1 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.

19. APPROVAL OF THE POLICY:

Document Name: Security Policy and Procedures

Signature

MUNICIPAL MANAGER

03 \ 11 \ 2017 .

Date:

FETAKGOMO – GREATER TUBATSE
LOCAL MUNICIPALITY

LC (FGTM) RESOLUTIONS	FILE NO. S																
TOWN	MEET NR	O C M	0	1	2017	TAKEN ON	2	6	1	0	2	0	1	7	ITEM	OC42	2017

JOB DISPOSAL		FOR INFORMATION
	MUNICIPAL MANAGER	
	DIRECTOR : BUDGET & TREASURY	
	DIRECTOR : CORPORATE SERVICES	
	DIRECTOR : COMMUNITY SERVICES	
	DIRECTOR : INFRASTRUCTURE, DEVELOPMENT & TECHNICAL SERVICES	
	DIRECTOR : DEVELOPMENT & PLANNING	
	DIRECTOR : LAND ECONOMIC DEVELOPMENT & TOURISM	
SUBJECT		
NR : OC42/2017	RESOLUTION **Reviewed Risk Management Policies, Strategies and Plans**	

Resolved

1. that Council approved the reviewed Risk Management Policies, Strategies and Plans :

   a) Risk Management Policy

   b) Risk Management Strategy

   c) Fraud Risk Management Policy

   d) Risk Management Charter Policy

   e) Security Policy

   f) Anti-Fraud and Corruption Prevention Policy

Date : 31/10/2017 **Chairperson of the Municipal Council** ____________