GREATER GIYANI MUNICIPALITY

INTERNAL SECURITY POLICY

VERSION 01

TABLE OF CONTENT

ACCROYNAMYS, DEFINATIONS AND SCOPE OF APPLICATION

(i) Acronyms used in this policy

COMSEC-Communication Security Agency

EXCO - Executive Committee of Council

GGM-Greater Giyani Municipality

SAPS-South African Police Service

SANDF- South African Defence Force

NIA- National Intelligence Agency

PSIRA - Private Security Industry Regulation Act

VIP-Very Important Person

(ii) Definitions

In this policy, unless the context otherwise indicates:-

"Access control" means a process in which several measures are applied to ensure that any object or person requiring access to premises of an institution, is safe, has a bona fide reason to enter, is entitled and authorised thereto, and that the institution or its staff will not be exposed to danger or to breaches of security during the presence of such a person or due to his/her gaining access.

"After hours" Means from 16:00 and 07:00 from Monday to Friday. Public holidays and weekends are also regarded as after-hours.

"Accounting Officer" means the Municipal Manager

"Applicant" means any person whose security competency is being investigated.

"Crime" means an unlawful human conduct which is performed with a blameworthy state of mind and which is punishable by the state. From a sociological view, crime is an anti-social conduct which is viewed as unacceptable by the community

"Deliberate theft" means this is where the individual (employee) steals from his employer for his/her personal gains. This will include laptop thefts (red flag) and other types of items that can be stolen for personal gains

"Dangerous Object" means any explosives or incendiary material/device, any firearm and any gas, weapon, or other article ,object or instrument which may be

employed to cause bodily harm to a person, or to render a person temporarily paralyzed or unconscious or and to cause damage to property

"Declaration of Secrecy" means an undertaking given by person who will have, has or had (Confidentiality Agreement) access to classified information, that he/she will treat such information as secret. Access will be defined by the nature of the office, the occupied position and by being a staff member of GGM

"Employee" means any person appointed by GGM which includes:

- Permanent staff /Temporary or casual staff/ Contract staff
- Contractors/Consultants

"Municipal security" means the department ability to preserve its core values/ existence, to defend itself from potential attackers or to have a strong security system / capability to match or deter the power of internal and external environments against the probability of damage.

"Investigation" means systematic searching for the truth and gathering of valuable facts/information;

"Physical Security" means that condition which is created by the conscious provision and application of physical security measures for the protection of personnel, property and information;

"Security" means that condition free of danger created by the conscious provision and application of security measures;

"Security Officer" means the authorized officer appointed by the GGM (custodian of GGM premises), in terms of section 2(2) of the Control of Access to Public Premises and Vehicle Act, 1985. He/she is responsible for security functions

"Security Area" means any area to which the general public is not freely admitted and to which only authorised persons are admitted;

"Security Audit" means that part of security control undertaken to:-

- ❖ Determine the general standard of 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 regarding security problems experienced; and
- ❖ Encourage a high standard of security awareness;

"Security Registers" means any document specified for recording of security status, incidents and classified documents e.g. Key Control Register.

"Firearm," which includes:-

- Any device that can "propel a bullet or projectile through a barrel or cylinder by means of burning propellant.
-

"Official hours "shall mean 07:30 – 16:00(let's consider 07:00-16:00) to be the opposite of after hours

"Opportunist theft" means the kind of theft occurs when a person happens to be in the right place at the right time and takes the opportunity to steal something which has been left unprotected because the opportunity to steal has been created. This occurs as a result of poor office security e.g. laptop theft.

"Premises" means any building, structure, hall, room, and office which is the property of the GGM or occupied by its members who has right to access.

1. OBJECT OF THE POLICY

The purpose of this policy is to lay down a set of security rules by which all employees of Greater Giyani Municipality, visitors and service providers must abide. These rules will guide employees, visitors and contractors in physical security within the municipality

The primary purpose of a physical security policy is to inform staff and managers of those essential requirements for protecting the assets of the institution, of which the most important are people, property and information. This policy will specify the mechanisms through which these requirements can be met.

2. LEGISLATVE FRAMEWORK

The internal security policy is derived from the following legislations:

(1) Constitution of the RSA, Act 108 of 1996

The Constitution of the Republic of South Africa, as the supreme law of the land, regulates and limits the practice and conducts of security. All security policies and prescripts must be given within the provisions or framework of the Constitution, and must fully comply with the letter and the spirit therefore. Amongst others:

- Chapter (Bill of Rights)
- Section 13 (Right to Privacy)
- Section 36 (Limitation of rights)

(2) Criminal Procedure Act, Act 51 of 1977

The Act consists of all legal rules, which stipulate what human conduct is punishable by the state, and lays down the form of punishment that may be given to an offender. It prohibits certain conduct, and imposes a duty on members of society to act in a certain manner. The law lays down the procedure the state has to follow in order to punish the offender. A security component (officer) uses this act to enforce the law and protect the lives of personnel, information and property. Amongst others:

- Section 24 (search of premises)
- Section 23 (search and seizure)
- Section 28 (decency in searching)

(3) Control to Access to Public Premises and Vehicles Act, Act 53 of 1985

Access to Public Premises and Vehicles Act, requires heads of institution to safeguard buildings or premises occupied or used by or under the control of

government for the protection of the people therein or thereon, and for matters connected therewith.

In terms of the MISS (Chapter 8 (1) (1.3)) Heads of institution (Accounting Officer) is responsible for the enforcement of the provisions of the Control of Access to Public Premises and Vehicles Act (Act 53 of 1985) for the purpose of safeguarding buildings or premises occupied or used by or under the control of municipality.

(4) Municipal Finance Management Act, Act 10f 1999

To regulate financial management in the local sphere of government; to ensure that all revenue, expenditure, assets and liabilities of municipalities are managed efficiently and effectively; to provide for the responsibilities of persons entrusted with financial management and to provide for matters connected therewith

(5) Occupational Health and Safety Act, 1993 (Act 85 of 1993)

The Act provides for the obligation of the employer and employees to promote occupational health and safety. Division of Security Management is charged with responsibilities of co-coordinating the activities of departmental Health and Safety Committee for the implementation of this Act. It regulates the employer to ensure the provision of a safe working environment that is free of hazards.

(6) Firearms Control Act 60 of 2000

It regulates and provides control measures over firearms

(7) Trespass Act, 1959 (Act 6 of 1959)

This Act addresses the procedure and specification to be taken against persons who unlawfully obtain access to GGM Premises.

(8) Security Officers Act, 1987 (Act 92 of 1987) read with Private Security Industry Regulation, Act, 2001 (Act 56 of 2001)

The Act provides for the establishment of the Security Officers Board, whose main function is to exercise control over the occupation of security officers and to maintain, promote and to protect the status of the security occupation. It also provides for application procedure for registration as security officers, disqualifications and withdrawal of registration by Board, and a code of conduct for security officers.

3. POLICY APPLICATIONS

This policy applies to all municipal security personnel, all municipal employees, councilors and visitors.

4. SECURITY STRUCTURES, OFFICES, RESPONSIBILITIES AND DELEGATIONS

(1) **The Accounting Officer**:

(a) Designate an official to manage security issues within the municipality.
(b) Ensure and oversee the development, implementation and maintenance of an internal security policy for the municipality that complies with all the requirements of the MISS.
(c) Ensure that training and awareness programmes are implemented in the institution to sensitise employees and relevant contractors and consultants of the institution
(d) Ensure that individuals who have specific security duties receive appropriate training related to those duties.
(e) Ensures that all breaches of security are dealt with.
(f) The authority and responsibility for the drafting of instructions, prescripts and procedures for approval by the Accounting Officer and determining of the security needs of the GGM is delegated to the Director Corporate Services.
(g) All members of staff are, however, expected to lay a role in ensuring that visitors or clients, information and other assets are secure at all times. Frequent efforts shall, therefore, be made to raise conscious level amongst the staff on the importance of security and the strict execution of the security prescripts (policy).

(2) **Sub-Directorate: Physical Security**

The purpose of the sub-division: Physical security is to develop, implement and evaluate policy, practices, code of ethics, procedures and guidelines in respect of physical security risks.

5. PHYSICAL SECURITY

(1) The GGM is threatened by a variety of risks, which are aimed at its staff members, buildings, property or information. As part of the total counter intelligence process, steps or actions are taken also on the terrain of physical security, not only to defend against these threats, but also to limit the damage in case of an incident (which may include a breach of security of any kind), and to facilitate the eventual investigation into the incident.

(2) The GGM values the safety of its employees, property, contractors and visitors.

Bearing in mind the financial limitations of the implementation of physicals security measures,

greater emphasis is placed on employee participation to help accomplish a security working environments. Compliance with the applicable security prescripts will help to achieve the intended security objectives.

(3) The purpose of physical security include the following:

(a) To deter an intruder from entering the municipal premises
(b) To detect the attempted entry or presence if an intruder succeeds in penetrating
(c) To limit the harm that can be done if an intruder has managed to gain entry without being detected, using measures such as locks, keys, strong rooms, safes and other physical barriers.
(d) To detain the intruder by using silent alarms or security patrols

(4) **Access Control**

(a) Access control will be performed by in-house security personnel.
(b) The authority for the application of access control measures is derived from the Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985).
(c) No persons shall, without the permission of an authorized security officer, enter any of the buildings occupied by GGM

(5) Municipal property

(a) All private property, e.g. computer equipment, cameras, recording devices, radios and kitchen equipment etc., brought onto Municipal premises must be declared to the security personnel at the reception desk. In case of the removal of municipal property a removal permit approved by the Manager Assets shall be completed and handed out at the security checkpoint.

(6) **Visitors**

(a) All visitors must comply with the provisions of the Control of Access to Public Premises and Vehicles Act (positive identification by means of a green identity document, driver's licenses and/or passport). Every visitor must positively identify himself or herself at the access control point of the municipality. Persons refusing to be subjected to the prescribed security procedures will not be permitted access to the premises. Visitors on municipal premises shall, at all times, obey lawful orders given by authorized officers.

(b) All visitors to Office bearers (i.e. Mayor, Speaker, Chiefwhip, full time councillors) and top management (i.e. Municipal Manager and Directors) must be escorted by the security officers, after the necessary access control logistics has been done. Under no circumstance will such visitors be allowed to go to those offices by themselves.

(c) The Security Manager may consider an exception to the rule for member of state security organs – SAPS, NIA SACSA, SANDF, VIP guests- provided that such persons are on official duties and provide positive identification and /or appointment certificate. In case of private visits, such officials shall be handled as visitors.

(d) The security principle of "No identity, No entry" will be consistently applied and enforced by security officer. For the purpose of crime prevention and safeguarding human life, property and information, all visitors will undergo an electronic security examination mainly at Civic Centre which is the head office of GGM.

(7) **Contractors**

(a) All contractors who have not been issued with a municipal approved access card, desiring access to the premises, shall be registered as visitors subjected to the security measures as prescribed in the policy document.

(8) **Key control**

(a) The Security Manager as the Key Control Officer of the municipality will appoint an official in writing as a "key custodian" to manage and control all office keys of the respective municipal premises and a key register will be utilized for this purpose.

(b) Key control will only be the function of in-house security personnel.

(9) **Firearms**

(a) All municipal premises are declared "gun free" zones and no firearms will be permitted onto the premises, unless for those exempted (SAPS, SANDF and/or SASS)

(b) All firearms with the exception of those in the possession of authorized persons, e.g. police and other authorized officials, shall be handed in at security for safekeeping. All firearms must be recorded in a relevant firearm register. A firearm register must be signed by both the owner of the firearm and the security officer. A gun holding facility will be created to cater for such circumstances.

(c) Municipal firearms shall only be issued to officials who are in possession of a firearm license issued by the accredited Government agency (e.g. SAPS).

(d) The Section on Security Services will comply with the statutory requirements of the Firearms Controls Act when utilizing firearms. This will include

accreditation, licensing, shooting practice, reporting, safe-keeping, and controlling, safety precautions and inspections by the SAPS.

(10) **Physical Search**

(a) Section 13 (Right to Privacy) of the Constitution of the Republic of South Africa has been well-established in the Bill of Rights and subject to the limitation clause applicable. Rights to privacy can only be limited if the limitation is reasonable and justifiable in an open democracy based on human dignity, equality and freedom.

(b) Security officers should perform their duties as required by the security policy and one of their duties will be searching of persons. In realising the crime prevention and loss control strategies to all GGM offices, section on Security Services is committed to a zero tolerance with regard to theft or any criminal activity that may result in losses or intolerance to GGM.

(c) The Municipal Manager has a common law right, as the accounting officer of the municipality to safeguard the property of GGM and to achieve that duty all visitors, contractors, consultants, staff should be searched accessing in or out. Caution will be made to maintain the employer and employee relationship of trust and to act within the parameters of the Constitution. This right is not there in legislations and that does not make it illegal.

(d) The Municipal Manager as the accounting officer has the right to authorize the section on Security Service at any time to conduct searches on persons and vehicles at entrances and exit points, as and when required. The Municipal Manager can issue a directive for searching at any time as he so wishes.

(e) A search will always be a condition of access to GGM. The obvious objective is to prevent prohibited items from being introduced where they can be used to effect destruction and or theft of assets. Security officers will conduct searches on handbags, suitcase, and vehicle on a routine or random basis. Such searches will be conducted with consideration to human dignity.

(f) Security officer should take care that weapons are not taken into the building: fire
arms, explosives and any other dangerous objects which could be used to harm or damage. This include any object, apparatus or equipments or parts thereof which could be used to intercept, record, copy or reproduce information, other than that which is the property of GGM.

(g) Failure or refusal to abide or submit to security instructions or to declare any dangerous objects to security officers when requested to do so will be viewed as a breach of security and the visitor concerned will be denied access and removed from GGM premises. Resistance to removal of the visitor will be overcome with the use of reasonable minimum force and where necessary an arrest can be effected.

(11). **Contingency planning**

(a) A contingency plan shall be developed, approve and implemented. This plan shall be feasible and practiced regularly.

(b) All emergency exits in the buildings shall be used for the sole purpose of evacuation. Emergency exit doors are to be kept closed at all times.

(c) Emergency exits must be free of obstruction (e.g. furniture, vehicles etc).Use of emergency equipment (fire-hoses etc) for other non-emergency purposes (washing of vehicles etc) are prohibited.

(12) **Physical Security Appraisals**

(a) All GGM premises shall be subjected to a physical security appraisal before any security measures can be installed/implemented.

(b) The Manager responsible for security services may submit the physical security appraisals to the SAPS and NIA security advisory units for consideration and advice. The SAPS and NIA Security Advisory units may be requested to conduct physical security appraisals as and when deemed necessary.

(13) **After hour's access**

(a) All employees who require access or exit from the premises after-hours should positively identify themselves and subject to completion of the "After-hours register".

(b) No employees will be allowed to enter the premises after-hours if he or she is under the influence of liquor or any intoxicating substances. Such will incident constitutes a breach of security and it will be recorded in the necessary internal registers.

(14) **Fire detection and control**

(a) All fire detection equipment's and/or systems will be linked to the security control room and any tampering or misuse of fire fire-fighting equipments will be considered misconduct and will be punishable in terms of the Fire Brigade Act.

(b) All sensitive and/or restricted areas must be installed with the appropriate fire-fighting equipments and alarm system that are proactive.

(15) **Use of security registers**

(a) Registers are used as source of information during risk, threat and vulnerability analysis

(i) It can be presented to a court of law as evidence and in a disciplinary hearing
(ii) It can be an evaluation tool for section on security services effectiveness
(iii) It can be used to compile periodical security breaches statistics
(iv) It can serve as a deterrent for misbehaviour / misconduct of security personnel or staff
(v) It can also be used as a justification for certain security measures

(b) The following security registers shall be put in place:

NAME OF REGISTER	PURPOSE
Visitor register	To record all visitors, and contractors entering departmental premises.
After hours register	To record all officials visiting the department after hours (16h00 to 07h00)
Key register	To record keys issued to the official at first time.
Key control register	To record daily locking and unlocking of offices.
Firearm register	To record all private firearms
Occurrence Book (OB)	To record all security activities e.g. handing-over, inspection, patrols etc.
Asset removal permit	To record all equipment to be removed from the premises

NOTE: The above list will be amended, increased or reduced whenever a need arise.

(c) All security registers utilized within the municipality remains the property of the GGM.

(16) Access Control to Secure Boardrooms

(a) A boardroom is a restricted area; therefore strict access control shall be applied and enforced regarding access to "secure boardrooms".

(b) All boardrooms where sensitive information is discussed should be locked at all times and if the boardroom is not locked it constitute a breach of security and misconduct on the part of the responsible official.

(17) **Sweeping exercise**

A sweeping exercise will be conducted biannually in all areas where sensitive information is discussed and also upon request by the Municipal Manager or his delegate.

6. SECURITY SCREENING (Personnel Security)

(1) Security screening

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

(b) Security screening must be regarded as the basic line of defence that can be taken to protect classified and sensitive information.

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

(d) All personnel working in the Section on Security Services will be subjected to security vetting prior to taking up employment.

(e) The following employees shall be subjected to security screening before appointed i.e. the Municipal Manager, Directors, Managers, all security officials, all records management officials and any other employee which by the nature of the work the municipal manager may deem it necessary to subject such an employee to security screening

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

(2) Validity of Clearances of personnel and companies, consultants

(a) The respective security clearances for personnel shall be valid for the following periods:

Level of security clearance	Duration of clearance
Top secret	5 years
Secret	5 years
Confidential	10 years
Office bearers in ultra-sensitive posts	3 years or as and when required

(b) Security clearances for consultants and sole proprietorship are valid for the period of the project and once the project is finalized the clearance becomes invalid. The NIA will internally validate the security clearance for a period of one year and a request for extension of that clearance can be made by the client department.

(c) Security clearance for companies will be valid for the period of the project and once the project is finalized the clearance becomes invalid. The NIA will internally validate the security clearance for a period of two years provided that the profile of the company remains the same.

(3) **Upgrading of a security clearance**

(a) In case where an employee is appointed in a post that requires a higher level of security clearance, a security screening investigation shall be conducted before an upgraded security clearance may be issued

(b) The period of validity of the higher level of security clearance obtained in this way is calculated from the date the higher clearance is issued.

(4) **Oath of Secrecy or Non-disclosure agreements**

All officials, temporary workers, consultants and contractors shall sign an "Oath of Secrecy" document as defined in the Protection of the Information Act (84 of 1982) before assumption of sensitive duties within the Municipality In case of existing employees the Oath will be circulated to all.

(5) A Declaration of secrecy or an Oath of Secrecy form must be signed by all employees and one copy be filed in the Human Resource (personal file).

(6). **Appointment of foreign nationals**

The appointment of foreign nationals will be the discretion of the council.

7. BREACHES OF SECURITY AND INVESTIGATION

(1) All security breaches, potential or alleged security breaches must immediately be reported to the manager responsible for security services or security control room. Among others, security breaches shall mean the following:

(a) Leakage of sensitive information; wittingly or unwittingly
(b) Burglary, robbery, assault, pointing of a firearm
(c) theft of municipal property
(d) intimidations
(e) loss of access cards or keys
(f) threats (telephonic, verbal and/or physical)
(g) Any malpractice that may have a potential to cause harm to human lives, damage to assets etc.
(h) suspicious objects and/or unknown person wandering around the premises
(i) ex-employees (fired) or employees on suspension wandering in the premises

(2) All security breaches must within 48 hours be reported to the nearest South African Police Services and immediately to Manager responsible for security services.

(3) An affidavit with full descriptions surrounding the circumstances which led to the loss and particulars of equipment (e.g. model, serial numbers etc.) must be indicated and the case number and investigating officer of SAPS must be forwarded to the Manager responsible for security services.

(4) The reporting protocols: all security breaches will be reported to the Manager responsible for security services or his delegate and the Manager responsible for Security Services and/or his delegate will: as follows: Manager responsible for Security Services will liaise with

(a) in case an incident constitute a breach of security where sensitive information is lost, stolen and/or tampered with, the incident should be reported to the NIA.
(b) In case an incident is of a criminal nature, it should be reported to the SAPS
(c) In case where an incident involves theft of cryptographic equipments, it should be reported either to Comsec and/or SACSA. The NIA must also be notified of the incident and it should also be reported to SAPS because theft is a criminal offence.

(5) The purpose of internal investigation is not to only to determine what went wrong or to identify the wrongdoer but also to identify vulnerable areas, to assess the damage, determine which specific measures were not adhered to or not effective or even absent. Further, internal investigations are conducted to recommend appropriate security countermeasures and internal control systems to avoid recurrence of the security breach.

(6) Breaches of security must always be dealt with the highest degree of confidentiality in order to protect the official(s) concerned and to avoid divulgence of sensitive information.

(7) The Manager responsible for Security Services will report internally all security breaches to the Director Corporate Services.

(8) All investigations should be conducted within the ambit of the Constitution of the Republic of South Africa (Bill of Rights) and/or the Criminal Procedure Act.

(9) The municipality may outsource the services of a private investigator or investigator from other government department or government agencies to conduct investigation within the municipality.

8. OFFICE SECURITY

(1) Each official in the GGM is responsible for the security of his/her office, apart from the security measures provided by the security component.

(2) Office keys must be kept in officials possession at all times.

(3) Visitors must not be left alone in offices and must be kept under constant supervision whilst on the premises.

(4) All employees should ensure that their offices are locked at all times if they move out of the office, even for a short period. This aims at preventing or limiting the theft of private items (cellular phones, handbags) and other state property including laptops etc.

(5) Offices, cabinets, desk drawers, safes and/or strong room keys where sensitive information or property is stored must not be left hanging on doors, cabinets, desk drawers, safes and/or strong rooms, or hidden in pots plants. Such keys must be kept in the possession of the employee at all times.

(6) All electrical equipment such as computers, printers, copier machines, heaters and lights must be switched off before leaving the office as well as closing of windows especially during the nights and weekends.

(7) **In case of closed office plan**: At the end of the working day (knock-off time), before leaving, all employees should ascertain that:

(a) Lights and electrical equipment's are switched off
(b) Blinds and curtains closed / drawn in
(c) Doors/ windows/ safes and cabinets are closed / locked
(d) No cigarette, tobacco or matches left burning

(8) Human Resource Management shall advice all employees during induction that GGM is not responsible for any loss or damage in respect of private property.

(9) Any theft of GGM property in offices including laptops will be investigated by the relevant structures and if the fault was on the part of the employee, who fails/neglect and/or refuse to uphold certain security measures of those properties or items, they will be held liable for the loss.

(10) Occupants of offices where classified or sensitive matters are dealt with must always be present when artisans, technicians or cleaners are performing their duties in such offices. Special care must be taken on such occasions to ensure that they do not gain access to classified matters.

(11) **After Hours Inspection**

(1) The security officials will conduct after-hours inspection in all the office within the GGM to ensure adherence and compliance to Office Security.

9. SECURITY COMMITTEE

(1) GGM INTERNAL SECURITY COMMITTEE

(a) The Manager responsible for security services is responsible for the establishment of the GGM Security Committees. The approval for the appointment of the members shall be obtained from the Municipal Manager.
(b) The main responsibility of the Security Committee is to consider, co-ordinate and monitor the formulation and implementation of the security policy, conduct an annual review on the policy and also recommend changes where and when necessary.

(2) CCOMPOSITION OF THE SECURITY COMMITTEE

(a) The Committee shall comprise of seven members (i.e Manager Administration as the Chairperson, Protocol and Security Officer as the Secretariat, Risk Officer, I.T manager and representation from each municipal departments).

(3) The functions of the Committee are as follow:

(a) Identify any security breach that have taken place in the past resulting in the unauthorized access to, disclosure, loss or destruction of information and assets that is held by GGM and requires protection

(b) Conduct ongoing assessment of security threats, risk and vulnerabilities to determine the necessity of implementing supplementary counterintelligence measures that will reduce the risks to an acceptable level.

(c) Analyze the audit report and the institutional risk register and recommend remedial actions.

(d) Consider and evaluate the implementation of the policy and where necessary make inputs for amendment of the policy

(e) Make recommendations on the security projects and budgeting.

(f) Quarterly security report to be presented and discussed.

(g) Ensure the communication of the approved policy to all staff members and relevant consultants and contractors.
(h) Make recommendations on any matter relating security service of the municipality.

(4) **MEETINGS OF THE COMMITTEE**

(1) Meeting of the security committee should be convened once per quarter.
   (a) The Manager Administration should preside over the meeting.
   (b) Minutes of the meeting should be compiled by the Protocol and Security Officer
   (c) The quorum of the meeting should be constituted by at least 50+ 1 of the members who constitute the committee.
   (d) Discussions of meetings remains confidential
   (e) Members of the committee will sign a declaration of oath of secrecy.

10. SECURITY TRAINING AND AWARENESS

(1) Development of training and awareness programmes

   (a) The Manager responsible for security services of GGM and the Training Division of the municipality will be responsible for the development and implementation of security training and awareness programmes for the GGM security officials.

11. DEFAULT:

(1) There is no point of making laws or policies if people are allowed to ignore them and continue with deviations that impact negatively on the municipality. All employees, contractors, consultants of the GGM must uphold the provisions of the internal security policy.

(2) The GGM will take all reasonable practical steps to ensure that the security requirements are communicated and implemented in the municipality to avoid non-compliance.

(3) GGM cannot ignore or tolerate non-compliance of the security policy by employees, contractors and/or visitors in any area. This includes the employee's, contractors, visitor's refusal or negligence to implement security requirements within the GGM.

(4) Failure to comply with this policy is an offence of which the municipality may subject any person who default to punishment or re-imbursement of the lost costs.

12. IMPLEMENTATION AND REVIEW OF THE POLICY

(1) Implementation

The policy shall commence immediately after signed by the Mayor.

(2) Review of the policy

The policy shall be reviewed on recommendation by the security committee whenever a need to do so arise.

Signed by ZITHA T

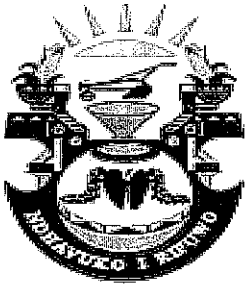
MAYOR: Zitha T. _____ _____ 17/05/2024

SURNAME & INITIALS **SIGNATURE** **DATE**

COUNCIL RESOLUTION:CR 164-17/05/24SP

FORM A (Employees)

GREATER GIYANI MUNICIPALITY



OATH OF SECRECY

I, the undersigned _____
(Full names & Surnames)

Employed as (Designation) _____ By the Greater Giyani Municipality.

I do hereby make oath and say: I know and understand that, I am required to keep any confidential information to myself and to disclose it, only under ether of the following:-

(i) when required by a court of law,
(ii) when authorized by the Municipal Manager or by an officer authorized by him/ her to grant such permission,

Further, that I understand that, failure to observe the provisions of the Protection of Information Act may result in corrective measures taken and shall be guilty of an offence.

I am aware and have taken cognisance of the possible consequences that may form any breach or contravention of said provisions and instructions.

_____ _____
DEPONENT DATE

FORM B (contractors/consultants/service providers)

GREATER GIYANI MUNICIPALITY

NON – DISCLOSURE AGREEMENT

I,_____ OF I.D NO._____
(Full names)

On behalf of (Name of Business)_____

solemnly declare that:

1. I have taken note of the provisions of the Protection of Information Act (Act 84 of 1982) and in particular the provisions of section 4 of the Act;

2. I understand that I shall be guilty of an offence if I reveal/ disclose any information which I have in my disposal by virtue of the contract awarded to me/my company and concerning which I know or should reasonable know that the security or other interests of the GGM and the Republic require that it be kept secret from any person(s) or body other than a person(s) or body :-

   (i) to whom I may lawfully reveal it, or
   (ii) to whom it is my duty to reveal it in the interests of the GGM and/or the Republic, or
   (iii) to whom I am authorized by the Municipal Manager or by an officer authorized by him to reveal it

3. I understand that the said provisions and instructions shall apply not only during my tenure of the project but also after the completion of my project and/or on termination of my service with the GGM, provided that this restraint does not limit, my right to apply my trade in terms of the Constitution;

4. I am fully aware of the serious consequences that may follow any breach or contravention of the said provision or instruction;

(Signature)_____

(Place)_____

(Date)_____

Witnesses' 1 _____ _____
(Name) (Signature)

2. _____ _____
(Name) (Signature)