

## MSUNDUZI MUNICIPALITY



<b>Policy Name</b>	<b>SECURITY MANAGEMENT FOR COUNCILLORS AND STAFF</b>
<b>Policy Number</b>	
<b>Status (Approved policy)</b>	Approved
	Date: 31 January 2024
<b>Checked by Organizational Development Unit:</b>	Name: Nosiphiwo Cebekhulu
	Date: 06 September 2023
<b>Approved By</b>	
<b>Date Approved</b>	
<b>Date Last Amended</b>	
<b>Date for Next Review</b>	
<b>Date Published on Intranet</b>	
<b>Policy Author/ Champion</b>	Mr. Lulamile Mapholoba
<b>Policy Author Contact Details</b>	033 392 2056

## **TABLE OF CONTENTS**

<b>No.</b>	<b>CLAUSE</b>	<b>PAGE NO.</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>3</b>
<b>2</b>	<b>POLICY PURPOSE</b>	<b>3</b>
<b>3</b>	<b>DEFINITIONS</b>	<b>3 – 5</b>
<b>4</b>	<b>LEGISLATION AND SUPPORTING DOCUMENTS</b>	<b>5</b>
<b>5</b>	<b>STATEMENT OF INTENT</b>	<b>6</b>
<b>6</b>	<b>POLICY OBJECTIVES</b>	<b>6</b>
<b>7</b>	<b>POLICY APPLICATION</b>	<b>6</b>
<b>8</b>	<b>PROCEDURE/STRUCTURE</b>	<b>6 – 18</b>
<b>9</b>	<b>ROLES AND RESPONSIBILITIES</b>	<b>19 – 21</b>
<b>10</b>	<b>APPEAL PROCESS/GRIEVANCE PROCEDURE</b>	<b>21</b>
<b>11</b>	<b>MONITORING AND EVALUATION</b>	<b>22</b>
<b>12</b>	<b>POLICY REVIEW DETAILS</b>	<b>22</b>
<b>13</b>	<b>DATE OF IMPLEMENTATION</b>	<b>22</b>

## 1. **INTRODUCTION**

Safety and Security at the workplace is important for Councillors and Employees to perform their duties diligently and to the best of their ability. Any threat creates uncertainty and anxiety which negatively impacts the execution of Council duties. Therefore, Council has a responsibility to create a safe and secure environment for Council and its Employees. This is in line with the Msunduzi Municipality's vision 2040; To be a safe, vibrant, sustainable, and smart metropolis. The security of human resources is as important as the security of Council's tangible and intangible assets.

## 2. **POLICY PURPOSE**

- To provide a localized regulatory framework for the security of Councillors and Staff.
- To promote a safe and secure environment for personnel to perform their duties.
- To ensure efficient and effective security management.

## 3. **DEFINITIONS**

Term	Definition
Access Control	A process by which access to a particular area is controlled or restricted to authorized personnel only, as defined in the control of access to Public Premises and Vehicle Act No. 53 of 1985.
Security	A condition free of risk or danger to lives, property and information created by the application of protective security measures.
Security area	An area to which the public is not freely admitted, and to which authorized persons are admitted.
Councillor	A member of the Municipal Council.
Security vetting	The systematic process of investigation that is followed to determine a person's security competence.
Premises	Any sites, place or location regardless of whether it is or forms part of any temporary or permanent structure, and property that is owned by the Msunduzi Municipality.

<b>Term</b>	<b>Definition</b>
Municipal vehicle	Any vehicle which is the property of the Msunduzi Municipality and executing functions of Council.
Driver	A natural person employed by the Msunduzi Municipality to perform duties of driving a municipal vehicle and that is competent as per the National Road Traffic Management Act 93 of 1996.
Investigator	An internal investigator conducting normal and reasonable investigations for the interest of the Msunduzi Municipality.
Clearance certificate	A certificate issued to a person by the security confirming security competence of such person.
Office	A workspace utilized by the employees including storeroom and filling areas.
Security Breach	The negligent and/or intentional transgression of /or failure to comply with the prescribed security measures by a person(s) who has (have) been cleared and authorized to have access to classified or sensitive information.
Risk	The probability that injury or damage or unauthorized disclosure of information will occur.
Security officer	Any natural person employed by the Msunduzi Municipality to carry out security duties entitled to receive remuneration and benefits for rendering such service.
Visitor	A person who goes to see another person or a place for a short time.
Weapon	An instrument designed, used or usable for inflicting bodily harm.
Bodyguard	A person or a group people employed to protect someone from danger.
Mayor	Means a mayor or executive mayor of a category “A”, “B”, or “C” municipality unless the context indicates otherwise.
State Secret	Information which pertains to the affairs of a country and access to which is restricted by the government.

Term	Definition
Trade Secret	Trade secrets are intellectual property (IP) rights on confidential information which may be sold or licensed. In general, to qualify as a trade secret, the information must be: <ul style="list-style-type: none"> <li>• <b>commercially valuable</b> because it is secret,</li> <li>• be known only to a <b>limited group of persons</b>, and</li> <li>• be subject to <b>reasonable steps taken</b> by the rightful holder of the information to keep it secret.</li> </ul>
Personal Information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Shared Information	Information exchanged between various organizations, people, and technologies.
Confidential	Containing information whose unauthorized disclosure could be prejudicial to the municipal interest.
Top Secret	Containing or being information, whose unauthorized disclosure could result in exceptionally grave danger to the Msunduzi Municipality.

#### 4. **LEGISLATION AND SUPPORTIVE DOCUMENTS**

- Municipal Structures Act 117 of 1998
- Municipal Systems Act 32 of 2000
- National Strategic Intelligence Amendment Act 67 of 2002
- Minimum Physical Security Standards (MPSS) booklet, 2009
- Minimum Information Security Standards (MISS), 1996
- Protection of Information Act 84 of 1982
- Protection of Personal Information Act (POPI), 2013
- KwaZulu Natal Department of Cooperative Governance and Traditional Affairs- MG & A Circular No. 2 of 2023
- Remuneration of Public Office Bearers Act, 1998
- South African Local Government Association – Handbook for Municipal Councillors.

## **5. STATEMENT OF INTENT**

Msunduzi Municipality is fully committed to providing a safe and secure environment for both Councillors and Staff, and to ensure legislative compliance in the execution of this function.

## **6. POLICY OBJECTIVES**

The objectives of the Security Policy for Councillors and Staff is to:

- 6.1. Promote a safe and secure workplace environment.
- 6.2. Provide necessary mechanisms to ensure the safety of Councillors and Staff.
- 6.3. To protect personnel in the execution of their duties should a challenge arise during the performance of their tasks.
- 6.4. To secure the information and assets of the Msunduzi Municipality against identified threats according to baseline security requirements and continuous Risk Management.

## **7. POLICY APPLICATION**

This policy is applicable to all members of the management, employees, consultants, contractors, councillors, visitors, and any other service provider of Msunduzi Municipality.

## **8. PROCEDURE/STRUCTURE**

### **8.1. Security Incident/Breaches Reporting Process**

- 8.1.1. Whenever Msunduzi Municipality employees or councillors 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 Deputy Municipal Manager: Community Services.
- 8.1.2. The Deputy Municipal Manager: Community Services shall report all cases or suspected cases of security breaches for investigation to the appropriate authority of the institution.
- 8.1.3. The Deputy Municipal Manager: Community Services shall ensure that all employees and councillors are informed about the procedure for reporting security breaches.

- 8.1.4. The 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.

## **8.2. Categorization of Information and Information Classification System**

- 8.2.1. The Deputy Municipal Manager: Community Services must ensure that a comprehensive information classification system is developed and implemented in the institution.
- 8.2.2. All sensitive information produced or processed in the 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.
- 8.2.3. All sensitive information must be categorized into one of the following categories:
- State Secret
  - Trade Secret
  - Personal Information
  - Shared Information
- 8.2.4. Subsequently classified according to its level of sensitivity by using one of the recognized levels of classification:
- Confidential
  - Secret; and
  - Top Secret

## **8.3. Who to Protect**

- 8.3.1. All councillors and employees including their property and family members who are staying with the councillor, or an employee concerned during the time of threats or actual attacks.

## **8.4. Protection Guidelines**

- 8.4.1. Protection provided includes, inter alia, escorts, evacuations, armed response, Adhoc patrols and guards, depending on the nature of the threat or attack subject to funds available in terms of the Municipality's annual budget.

8.4.2. No firearm will be issued to any Councillor or employee under threat or attack.

8.4.3. Threats or attacks should relate to the Councillor's or employee's Council duties.

## **8.5. Risk Analysis**

### Councillors:

8.5.1. The Office of the Speaker should conduct a risk analysis profile of all Councillors to determine the levels of risk each Councillor is exposed to.

8.5.2. The Office of the Speaker should undertake the risk profiling in consultation with the SAPS, National Intelligence Authority, Municipality's Law Enforcement, and leaders of structures in the wards as well as social organizations within the communities.

8.5.3. The risk analysis should be comprehensive and should factor in the levels of responsibility given to Councillors in their respective areas.

### Employees:

8.5.4. The Senior Manager: Public Safety should conduct risk analysis for employees that might be exposed to any form of risk.

8.5.5. The Senior Manager: Public Safety should undertake the risk profiling in consultation with the SAPS, National Intelligence Authority, and Municipality's Law Enforcement.

8.5.6. The risk analysis should be comprehensive for improved risk mitigation or elimination.

## **8.6. No Insurance**

8.6.1. This policy or its provisions must not be interpreted or regarded as an insurance to the employee's or Councillor's life, or his/her property in cases of attacks leading to death or property damage.

8.6.2. Employees and Councillors are, accordingly, advised to secure their own insurances in this regard.



## **8.7. Protection of the Mayor and Speaker**

- 8.7.1. The Mayor and Speaker are entitled to two bodyguards each.
- 8.7.2. Deviation from the norm must only be based on the recommendations from the South African Police Service (SAPS).
- 8.7.3. The escorts will accompany the Mayor and Speaker to all official and private functions and may remain with at the respective places of residence after hours.
- 8.7.4. In cases of emergency or where a significant additional threat has been established, the Mayor and/or the Speaker may request additional security personnel. However, prior to the allocation thereof, the necessary investigations shall be concluded.
- 8.7.5. In the event of an emergency situation arising, the escort shall take immediate steps to ensure the safety of the Mayor and/or the Speaker and advise the respective control centres who shall in turn advise the SAPS of the situation but shall take no further action, unless the SAPS fails to respond.
- 8.7.6. The Control Centre shall in the first instance contact the SAPS and thereafter the Deputy Municipal Manager: Community Services who shall keep the Municipal Manager informed of all aspects of any particular threatening incident.
- 8.7.7. The guarding service provider is required to always maintain continuous communication with the SAPS in respect of VIP security.

## **8.8. Protection of Councillors**

Protection will be provided to any Councillor when under threat subject to the following procedure:

- 8.8.1. Such threats being reported to the Councillor's caucus leader, whose duty it will be to in turn notify the Municipal Manager.
- 8.8.2. Prior to the approval of such security arrangements, a risk assessment be carried out by the SAPS, the official responsible for Councillor support (Chief Whip), the Municipal Manager and any other such structures as may be considered relevant.
- 8.8.3. If the application is well motivated and an imminent life-threatening situation exists, security must be provided to the Councillor by the SAPS in the interim period while the assessment is taking place at the discretion of the Municipal Manager.
- 8.8.4. The period for which the security is provided is dependent on the outcome of the assessment referred to in 8.8.3 above.

## **8.9. Protection for Employees**

Protection will be provided to any employee when under threat subject to the following procedure:

- 8.9.1. Such threats have been reported to the immediate supervisor, whose duty it will be to in turn notify the Municipal Manager.
- 8.9.2. Prior to the approval of such security arrangements, a risk assessment be carried out by the SAPS, the official responsible for the immediate supervisor, the Municipal Manager and any other such structures as may be considered relevant.
- 8.9.3. The period for which the security is provided is dependent upon the outcome of the assessment referred to in 8.9.2 above.

## **8.10. Authority for Approval of Service**

- 8.10.1. Only the Municipal Manager may approve the allocation of VIP escort protection including any related expenditure, or the discontinuance of the VIP escort protection which must be ratified by the Executive Committee (EXCO).
- 8.10.2. The final duration of the allocation shall be approved by EXCO having due regard to the outcome of the risk assessment referred to in 8.9.3 above, and it being noted that a periodical review may be undertaken.
- 8.10.3. All services shall be procured through an approved process in terms of the Council's Supply Chain Management Policy.

## **8.11. Provision of Drivers for the Mayor**

- 8.11.1. The Mayor in office shall be entitled to a chauffeuring service on a permanent basis.
- 8.11.2. Such service shall consist of one driver for an 8-hour shift and will be provided for in the Council's Organizational Structure.
- 8.11.3. The driver will accompany the Mayor to both official and private functions.

## **8.12. Office Security and Key Control (Staff Members)**

- 8.12.1. Each member is responsible for the inspection of his/her office or workstation for any signs of intrusion at the beginning of each day. If the member detects any signs

of intrusion, he/she should notify the immediate supervisor or safety officer so that the matter can be reported to the Manager: Security Services immediately.

- 8.12.2. Cleaning of offices for persons handling classified information should be done during official working hours and supervised by the occupant of the office. In the event of this not being possible and the office is occupied by the Mayor, Speaker, Chief Whip and Municipal Manager, the office should be cleaned under the direct and strict supervision of an in-house security officer. The occupants of offices that contain sensitive apparatus or documents, which cannot be hidden or locked away, may clean their offices themselves.
- 8.12.3. Key Control of the institution shall remain the responsibility of the Security Services under the appointed Key Custodian Officer as prescribed in the Minimum-Security Information Security Standard (MISS), to ensure effective key control within the municipality and all keys issued need to be registered in a “key register” which is to be maintained by the Security Officers.
- 8.12.4. The occupant of an office should lock the doors of the office or working area at all times when leaving such an office or working area.
- 8.12.5. Office keys should be safeguarded in such a manner that the keys are not lying around where the key number could be identified by any person with ulterior motives e.g. hanging in the door or left unattended on the table.
- 8.12.6. A “clean desk policy” should be adopted by all personnel ensuring that no sensitive, classified, and valuable assets are left unattended in any workstation.
- 8.12.7. Keys should not be duplicated without the knowledge of the Security Manager, or the relevant official appointed to be the key custodian.
- 8.12.8. At the end of the day, before departure, each official should ascertain that:
  - All electrical appliances are switched off.
  - No cigarettes, tobacco and/or matches are left burning.
  - Blinds/curtains are drawn.
  - Doors, windows, and cabinets are closed and locked.
  - Sensitive apparatus or documents are locked away.
- 8.12.9. A register with after-hours visitors to the Municipality should be kept and checked within 24 hours by the Manager: Security Services.
- 8.12.10. The jamming of doors fitted with electronic readers, either on the hallway or in offices is prohibited.

## **8.13. Types of Security**

### **8.13.1. Information Security: Categorization of Information and Information Classification System**

- 8.13.1.1. The Manager: Records must ensure that a comprehensive information classification system is developed and implemented in the institution.
- 8.13.1.2. 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.
- 8.13.1.3. Employees of the institution 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.
- 8.13.1.4. 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.

### **8.13.2. Physical Security**

- 8.13.2.1. Physical Security involves the physical layout and design of facilities of the Msunduzi Municipality and the use of physical security measures to delay and prevent unauthorized access to assets of the Municipality.
- 8.13.2.2. It includes measures to detect attempted or actual unauthorized access and the activation of an appropriate response.
- 8.13.2.3. Physical security also includes the provision of measures to protect employees from bodily harm.
- 8.13.2.4. Physical security measures must be developed, implemented, and maintained to ensure that the entire Municipality, its personnel, property, and information are secure.
- 8.13.2.5. These security measures shall be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Guard.

8.13.2.6. Msunduzi Municipality shall ensure that physical security is fully integrated early in the process of planning, selecting, designing, and modification of its facilities.

8.13.2.7. 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.
- Msunduzi Municipality will also ensure the implementation of appropriate physical security measures for the secure storage, transmittal, and disposal in all forms.

### **8.13.3. Information and Communication Technology Security**

8.13.3.1. Information and Communication Technology (ICT) security measures are essential in protecting confidential and classified information from unauthorized use, modification, loss and/or release.

8.13.3.2. ITC Security measures must be developed, implemented, and maintained to ensure that the entire Municipality, its personnel, property, and information are secure.

8.13.3.3. The Msunduzi Municipality shall:

- Ensure the implementation of an ICT Security System.
- Ensure that Approved ICT policies of Council speak to and promote ICT Security.
- All relevant systems will be secured as per ICT approved Policies of Council.

#### **8.14. Personnel Security Screening**

- 8.14.1. All newly appointed employees, councillors, contractors, and consultants attached to Msunduzi Municipality, who require access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security screening process.
- 8.14.2. 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.
- 8.14.3. 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.
- 8.14.4. This does not preclude re-screening on a more frequent basis as determined by the Accounting Officer, based on information which negatively impacts an individual's security competency.
- 8.14.5. Security clearances in respect of all individuals who have terminated their services with the Accounting Officer shall be immediately withdrawn.

#### **8.15. Identity Access Card Policy**

- 8.15.1. The access card is an integral part of any physical and technical access control system or procedure other than just being a means to positively identify departmental employees. The issuing and strict control of the identity cards is crucial for a safe and secure working environment.
- 8.15.2. Security Service is responsible for the manufacturing, issuing, and management of the Municipal identity access card.
- 8.15.3. The individual ID access card holders are responsible and accountable for their cards and how and where they are used.
- 8.15.4. Where external contractors are issued with the Municipal contractor cards, the line management by whom they are appointed is responsible for the control, use and return of the cards.

#### **8.16. Application for Identity Access Cards**

- 8.16.1. An identity access card shall only be issued on the strength of an application form that has been signed by both the applicant and his/ her Head of Department.

- 8.16.2. Application forms for ID access cards can be obtained from the Manager: Security Services.
- 8.16.3. Application forms shall be submitted at least 24 hours prior to the issuing of the card.
- 8.16.4. Once the employee's photograph and details have been printed onto the ID card, the relevant information will be captured into the access control system by the Manager: Security Services.
- 8.16.5. Contracted service providers and internship students must complete an application form for contracted staff.

#### **8.17. Recovery of ID Access Cards**

- 8.17.1. Human Resource Management shall recover the card from the employee whose employment with the Department has been terminated and submit it to Security Services within 24 hours of the termination of employment. Application for benefits of such an employment would not be processed before the card is returned.
- 8.17.2. Human Resources shall notify the Manager: Security Services on a monthly basis and in writing of the names and details of any person who left the Msunduzi Municipality during the preceding month. Upon receiving such notification, the Manager: Security Services will amend their records accordingly.

#### **8.18. Searching of Vehicles**

- 8.18.1. All Drivers of motor vehicles including employees, councillors must declare/disclose any dangerous objects constituted in terms of the Law and any property in their possession such as laptops before entering Municipal premises to the Security Officers.
- 8.18.2. The Security Officers must search the vehicle when entering or leaving to ascertain whether there is any Msunduzi Municipality Property that is being removed from Council premises without authorization. No employee shall without the permission of an authorized Security Officer enter with his vehicle for the purpose of parking inside the premises (Control of Access to Public Premises and Vehicles Act 53 of 1985). The Security Officers shall at any time remove such vehicle from any Municipal premises if it is considered necessary for the

safeguarding of the premises, its contents or for the protection of the people therein or thereon.

8.18.3. All vehicles for Councillors, employees shall have stickers identifying them for the purpose of allowing them inside the premises.

8.18.4. If Security Officers find anything that is unauthorized, it must be impounded, and the Municipal Manager be informed of such impoundment.

#### **8.19. Screening Of Employees And Service Providers**

8.19.1. The Msunduzi Municipality shall identify employees according to their scope of work who must undergo a systematic process to determine an individual's security competence before taking employment and security clearance be issued. This process will be done as mandated by the National Strategic Intelligence Amendment Act 67 of 2002, and the Security Manager shall be responsible for the screening process via the State Security Agency. Officials who have access to sensitive information shall undergo such screening and be issued with appropriate security clearance certificate before assumption of duties.

8.19.2. All service providers who have applied for job by tendering with the Msunduzi Municipality must be screened before the tender is awarded. A declaration of security clearance must be made on official forms by the Security before appointment.

8.19.3. General vetting of employees and management will only be done when mandated by the Municipal Manager.

#### **8.20. Control of Firearms**

8.20.1. The Security officers shall carry the firearms in a holster that is worn by or attached to his/her body and that a safety clip to lock in the firearm shall be provided and such a holster shall be concealed.

8.20.2. The following Municipal sites shall be declared "Gun-free zones"; therefore, the Gun Safe facilities shall be provided in the main entrance of respective sites; the Council Chamber, Halls, Water Treatment Centres, Revenue offices, Venues for Municipal, Provincial and National Events.

8.20.3. Officials and visitors in possession of firearms must leave them at the lockable gun deposit safes at the reception areas except close protectors of political



principals, SAPS and SANDF on official duties. The owner of the firearm will be required to produce a license for such a firearm before keeping it in the safe, and a record as prescribed by the Firearms Control Act no. 60 of 2000 be kept for the purpose.

#### **8.21. Institutional Events**

- 8.21.1. All institutional major events shall be coordinated with the involvement of the Manager: Security Services.
- 8.21.2. The Manager: Security Services must ensure that the personnel, VIPs, and all invited guests are safe and there is compliance regarding tight security measures in all events.
- 8.21.3. The institutional calendar of events shall be handed to the Manager: Security Services prior any planned event in order to prepare for security measures.

#### **8.22. Composition of the Security Committee**

- 8.22.1. A Security committee shall be established by the Municipal Manager, appointing the Director of the Department as the Chairperson of the Committee to ensure smooth running of the Security Services.

The committee shall be comprised of the following:

- (a) The Security Manager
- (b) IT Manager
- (c) Records Management Manager
- (d) Head of Disaster Management
- (e) Fire & Rescue Manager
- (f) Asset Manager
- (g) Transport Manager and,
- (h) Representatives from other Departments of the Municipality.

- 8.22.2. The Committee shall advise the Municipal Manager on matters relating to the Security of the Msunduzi Municipality.

The Committee shall:

- (a) Promote accountability and transparency in the Security Services.
- (b) Monitor the implementation of Msunduzi Security Policy.
- (c) Evaluate the functioning of the Security Services and report to the Municipal Manager.
- (d) Identify categories of information that require protection and components handling such information.
- (e) Identify the storage of information and who may require access to such information (internal/external).
- (f) Assist the Security Manager with conducting Threat and Risk analysis (TRA).
- (g) Assist security manager with the drafting and review of the Security Policy, Plans and Procedures.
- (h) Assist in awareness programs and the implementation of security measures.

### **8.23. Security Awareness**

- 8.23.1. The Security Manager shall be responsible for the execution of regular security awareness programmes to ensure that all personnel are security conscious. All personnel and interns will be required to attend the programmes and sign the attendance register. Managers will be required to release staff to attend such presentations.

## 9. ROLES AND RESPONSIBILITIES

Role	Responsibility
Employee	Report any threat directed to him/her to the immediate supervisor.
Councillor	Report any threat directed to him/her to the party caucus leader and to the Speaker
Supervisor/Manager	Report the threat to the Senior Manager: Public Safety and to the Municipal Manager.
Senior Manager: Public Safety	Conduct risk assessment and provide recommendations to the Municipal Manager.
Municipal Manager	The Municipal Manager bears the overall responsibility for implementing and enforcing the security program of the institution, towards the execution of this responsibility. The MM will also approve or not approve the allocation of a Bodyguard based on the risk assessment outcomes and availability of budget.
Deputy Municipal Manager: Community Services	<p>The DMM: Community Services shall:</p> <ul style="list-style-type: none"> <li>• Establish the post of the Security Guard and appoint a trained and Competent Security Guard in the post.</li> <li>• 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.</li> <li>• Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.</li> </ul>

Role	Responsibility
Head of Department	<p>The delegated security responsibilities lie with the respective Head of Department 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).</p> <ul style="list-style-type: none"> <li>• In the execution of his/her responsibilities, the Head of Department shall, among others:</li> <li>• Chair the Security Committee of the Municipality.</li> <li>• Draft the Internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of the Municipality in conjunction with the Security Committee.</li> <li>• Review the Security Policy and Security Plan at regular intervals.</li> <li>• Advise management on the security implication of management decisions.</li> <li>• Implement a Security Awareness Programme.</li> <li>• Conduct internal compliance audits and inspections at the Municipality at regular intervals.</li> <li>• Establish a good working relationship with the SAPS and liaise with the Institution on a regular basis.</li> <li>• As mentioned above the Head of Department should have delegated signing powers as per Municipal Manager's discretion.</li> </ul>
Line Managers	All managers in the Municipality shall ensure that their subordinates comply with this policy and the

Role	Responsibility
	<p>Security Directives as contained in the Security Plan of the Municipality.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• This includes the taking of disciplinary action against employees if warranted.</li> </ul>
Employees, Councillors, Contractors, Consultants, and other Service Providers	Every Employee, Councillor, Contractor, Consultant, and other Service Providers of the Msunduzi 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.
Stakeholders	<p>This policy is applicable to all members of the management, employees, consultants, contractors, councillors, visitors, and any other service provider of Msunduzi Municipality.</p> <ul style="list-style-type: none"> <li>• It is further applicable to all visitors and members of the public visiting premises of or may officially interact with the institution.</li> </ul>

#### 10. **APPEAL PROCESS/GRIEVANCE PROCEDURE**

Any dispute or concerns on the implementation shall be directed to the Municipal Manager in writing.

**11. MONITORING AND EVALUATION**

The Senior Manager: Political Support shall be responsible for the monitoring and evaluation of this policy.

**12. POLICY REVIEW**

This policy shall be reviewed annually in compliance with the necessary legislations and circulars from various government institutions.

**13. DATE OF IMPLEMENTATION**

This policy will come into effect on the date of adoption by Full Council.