UMZIMVUBU
LOCAL MUNICIPALITY

Enquiries: Bongile Ntlamba 039-254 6000 Reference: Date: 31/07/2017

To: MUNICIPAL MANAGER

SENIOR MANAGERS (HODs)
ASSISTANT MANAGERS
HEAD OF SECTIONS
ALL STAFF GENERAL

SECURITY DIRECTIVE: ACCESS CONTROL STANDARD OPERATING PROCEDURES FOR THE UMZIMVUBU LOCAL MUNICIPALITY PREMISES

1. Access control standard operating procedures for the Umzimvubu Local Municipality are hereby presented.

2. The standard operating procedure is informed by and complies with security legislation, national security policies (**MISS**) and minimum security standards (**Minimum Information Security Standard**).

3. The main objective of the access control standard operating procedure is to protect employees and Departmental institutions against security breaches.

4. The contents of the standard operating procedures shall be presented and clarified in Security Awareness and Training sessions.

5. Roles and responsibilities of categories of personnel in the municipality including all contracted service providers are highlighted.

6. Periodic security audits and inspections shall be conducted to determine and ensure compliance with the access control standard operating procedures.

UMZIMVUBU
LOCAL MUNICIPALITY

ACCESS CONTROL STANDARD OPERATING PROCEDURES

UMZIMVUBU LOCAL MUNICIPALITY

1. Introduction

The Umzimvubu Local Municipality Standard Operating Procedures prescribe security measures to counter threats and risks that can cause harm to employees, assets, critical information and operations of the municipality. The processes and procedures form part of the department wide operating systems, they provide assurance to service delivery commitments.

2. Scope

The standard operating procedures applies to,

2.1 All employees and temporary employees of the Umzimvubu Local Municipality,

2.2 All contractors, consultants delivering services to the Umzimvubu Local Municipality,

2.3 All movable property that is leased or owned by the Umzimvubu Local Municipality

3. Purpose

3.1 To set security standards for the Umzimvubu Local Municipality

3.2 To provide standard operating procedures for access control and asset movement

3.3 To provide responsibilities for monitoring, supervision and maintenance of the access control standards and asset movement

4. Legislative and Regulatory Provisions

The access control standard operating procedures comply with national legislation, national security policy and security standards, ULM security policy, associated security directives.

- Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985)
- Security Directive: Access Control at any ULM premises
- Notice: Security measures for departmental offices and institutions: Control of access to premises.

5. Access control

Access control is 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 *bonafide* reason to enter
- Is entitled and authorized thereto
- and that the institution and its employees 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.

6. Access Control Conditions

The conditions stipulated are provided for in security legislation, they are aimed at maintaining and improving security at the departmental premises, they should not be used to cause unnecessary inconvenience.

6.1 No visitor may be granted unconditional access to the offices of the municipality.

6.2 The person granted access must possess or display proof that the necessary permission has been granted

6.3 The persons on the premises with whom the visitor may not come into contact

6.4 The part of the premises which may not be entered upon (restricted areas)

6.5 The duration of presence on the premises

6.6 The escorting of the person concerned while on the premises

7. Granting of access

The granting of access to the premises of the ULM should be related to the functional activities of the ULM facility.

Functional activities are the following,

7.1 An employee reporting for duty

7.2 A visitor attending to the official functional activities of the ULM facility

7.3 All visitors must be escorted once access is authorized.

7.4 Security should be notified of any scheduled visits or deliveries.

8. Access Control Procedures

8.1 Identification

8.1.1 Access to ULM premises is granted on the basis of two forms of identification methods, that is positive identification and personal identification

8.1.2 Positive identification occurs when the visitor provides known forms of identification documents, which are;

8.1.2.1 RSA identity document, passport or drivers licence

8.1.2.2 South African Police Services (SAPS) or South African National Defence (SANDF), State Security Agency (SSA) or South African Secret Services (SASS), Traffic Officers and Law Enforcement Officer appointment certificate

8.1.2.3 Identity cards of other institutions are not acceptable as sufficient proof of identity.

8.1.3 Personal identification must take place when the visitor is not in possession of the above documentation to prove his identity.

8.1.3.1 The person visited must confirm the visit and the identity of the visitor.

8.1.3.2 A proper record of the visit is generated and kept, it should include; particulars of the visitor and the person visited, visitors address and the reason for the visit must be registered.

8.2.1 All employees and newly appointed staff should be provided with access control cards/ identifications cards to facilitate control of access to the premises.

8.2.2 Access control cards/identification cards must be prominently displayed at all times while on departmental premises.

8.2.3 Loss of the access control/identification cards must be reported immediately to security to prevent breach of security.

8.2.4 Employees must return identification/access control cards upon termination of service or transfer. In the event of death necessary means must be made to ensure return of the access control cards and assets.

8.2.5 All visitors, contractors, consultants and other service providers must be provided with the departmental identification cards in exchange for Republic of South Africa Identification Document, passport or drivers licence,

8.2.6 All access control cards must be returned to security at the end of each visit or duty in the ULM premises.

8.3 Security Registers

8.3.1 The purpose of keeping security registers is to ensure that in the event of emergency, accurate and relevant information of all personnel, visitors and service providers is available for identification,

8.3.2 Access control registers serve as proof that the visitor was granted access and authorized to be in the departmental premises

8.3.3 Assets and any other property taken out can be compared with any asset or property that the visitor brought in the premises

8.3.4 All records contained in relevant security registers must be kept in a secured storage at all times.

8.3. 5 Security supervisor must inspect security registers daily and provide a report to management for noting and action where necessary,

8.4 Escorting

8.4.1 Visitors

8.4.1.1 Visitors must be in the company of a person visited or a person from the same business unit at all times while within the premises of the department

8.4.1.2 The security official may, subject to the availability of security officers, escort a visitor to and from the host,

8.4.1.3 Visitors to Mayor, Speaker, Municipal Manager and HODs must be escorted upon arrival.
8.4.1.4 Do not carry the bags/luggage of the person being escorted.
8.4.1.5 Do not chat with the person escorted.
8.4.1.6 Maintain vigilance to counteract potential threats.

8.4.2 Deliveries, contractors and technicians

8.4.2.1 Prior arrangements should be made for all deliveries and contract work in the department

8.4.2.2 The relevant business unit where deliveries are expected or where contracted work has been requested should appoint a member from the business unit to provide escort for the duration of the service.

8.5 Access to Restricted Areas

8.5.1 Access to restricted areas such as server room, boardroom, registry, executive offices or any area designated as a restricted area, is limited only to authorized persons

8.5.2 The Municipal Manager or a person acting on his instruction can grant access to a restricted area

8.5.3 Contractors, consultants and other service providers must make prior notice and arrangements to gain access to restricted areas for the purpose of rendering a service,

8.6 After Hour Access Control Procedures

8.6.1 The Responsible Manager must inform security of any arrangements for officials to work after-hours in order to facilitate protection of staff and property.

8.6.2 In case of emergency all personnel that have gained access to the ULM premises must be identified

8.6.3 After-hour access control procedures and measures are applicable after normal working hours including weekends

8.6.4 A separate access control register must be completed by all officials that work after-hours

8.6.5 All the necessary particulars of an employee, time of entry and exit and the reason for working after hours must be entered in the after hour access control register.

8.6.6 After-hour access control register must be inspected during the tour of each security shift.

9. Searches

The purpose of conducting searches is to prevent prohibited items from being introduced into a ULM facility in order to prevent injury or death to employees, theft of assets or destruction of property.
The following objects are prohibited from the premises,

- Firearms, explosives, and any other dangerous object which could be used to cause harm or damage

- Any weapon, incendiaries (inflamatories), alcohol beverages, narcotics or controlled substance

- Any object, apparatus or equipment or parts which could be used to intercept, record, copy or reproduce information, other than that which is the property of the municipality.

- Only members of the SAPS are allowed to carry official firearms while on the premises.

Except for the members of SAPS, State Security Agency, the SANDF and our own traffic or law enforcement officers, any person who refuses to be subjected to search must be denied access to the municipal premises.

9.1.1 Entry Searches

9.1.1.1 Any person granted access to the premises must be requested to declare possession of the above prohibited items. Once declared

the unauthorized items must be retained at the security check/access control point for safekeeping.

9.1.1.2 Full particulars of the visitor and the details of the unauthorized object found must be entered in a relevant register and a receipt must be provided or other proof of seizure of such article, or access should be denied.

9.1.1.3 Any declaration, whether positive or negative should be followed by a physical inspection, search or examination by means of available technical aids.

9.1.1.4 In case of physical inspection, the visitor should open and show the contents of his/her jacket, bag, shopping bag or any other object.

9.1.1.5 Items and equipment such as laptops, projectors, and desktops must be recorded on the security register. Any item or equipment taken out by a visitor must be compared with what he/she brought into the premises.

9.1.1.6 As provided for in law a female visitor should be subjected to a physical search or inspection only by a member of the same sex.

9.1.1.7 If the premises are equipped with metal detectors they should be able to detect ferrous and non-ferrous metal with 90 percent effectiveness.

9.1.2 Exit Searches

9.1.2.1 The purpose of exit searches is to detect theft of assets or property.

9.1.2.2 As a general rule, everyone exiting the municipal premises should be searched.

9.1.2.3 Search is granted by the person leaving the premises.

9.1.2.4 Searches can be conducted manually or with the use of technical aids where these are available.

9.1.2.5 Where there are reasonable grounds that theft occurred and person refuses to be searched SAPS must be informed immediately.

9.1.3 Motor Vehicle Searches

9.1.3.1 As a general rule all vehicles should be searched prior to allowing entry and on exit from the premises

9.1.3.2 The only exception should be for emergency vehicles when responding to an emergency

9.1.33 Emergency vehicles should be recorded in the access control register after the fact,

9.1.4 Motor-Vehicle Search Procedures

9.1.4.1 Vehicle searches should include the boot, cargo space, undercarriage, passenger compartment at the minimum the engine

9.1.4.2 If many vehicles enter the ULM facility, random searches may be conducted

9.1.4.3 When vehicles are searched there should always be a security official observing the search process.

9.1.4.4 Items and equipment such as laptops, projectors, and desktops must be recorded on the security register. Any item taken out by a visitor must be compared with what was brought into the premises.

10. Asset Movement

The asset movement register must be used to record and maintain control of all movable assets between ULM offices and those taken out for repairs.

11. Key Control

11.1 Corporate Services must ensure that key control officers are appointed for respective sections.

11.2 All keys must be recorded in the key control register and be issued against a signature.

11.3 Any loss of keys must be reported immediately to Corporate Services to prevent breach of security. Replacement keys will also be recorded in the key control register and be issued against a signature

11.3 The key control officer must ensure that duplicate keys are available and kept in a secure facility (safe)

12. Security Breaches

12.1 A security breach is the negligent or intentional transgression of or failure to comply with prescribed security measures by a person who has access to classified or sensitive information,

12.2 Security breaches in which classified information or items were affected, lost, damaged or compromised must be reported to the Responsible Manager.

12.3 All security breaches constituting a criminal offence must be reported as prescribed above including SAPS for criminal, court directed investigations.

13. Specific Responsibilities

13.1 The Municipal Manager or his delegate must report to the State Security Agency all cases or suspected cases of security breach involving classified information for security investigation.

13.2 The Security Manager should conduct an assessment of the security breach and to provide recommendations in consultation with the State Security Agency.

13.3 All Responsibility Managers must ensure implementation of the access control procedures to protect ULM assets, systems and process; and report breaches of security. Immediate possession of all identification/ access control cards must be returned on transfer, termination of service or death of an employee.

13.4 Community Safety Department manages the security function at all ULM premises must ensure that supervision of the access control takes place on a day to day basis.

13.5 The On-Site Supervisor of a contracted security service provider must ensure that the management of the security function is adhered to as stipulated above.

13.6 Employees, contractors, consultants and other service providers must contribute to the maintenance of a safe work environment in the ULM premises by adhering to the access control procedures and its associated security directives.

13. Deviations

Deviations from the access control standard operating procedures will only be permitted in the following circumstances;

13.1 When security is breached in order to save or protect the lives of people

13.2 During unavoidable emergency circumstances, e.g., natural disasters

13.3 On written permission of the Municipal Manager, reasons for non-compliance to one or more aspects of the standard operating procedures shall be clearly stated in such permission.

13.4 Except for the above circumstances. Any other deviation must be reported to the immediate supervisor

14. General Patrols

a. Security personnel on duty during the day and night must patrol the entire building every 1 hour.

b. All patrols conducted must be clearly recorded in the occurrence register. The Security personnel must inspect the following areas:

- Obstacles on passages and escape route.
- Assets and information left unattended.
- Unlocked offices and cabinets.
- Leakages, fire equipment and lift lobby.
- Gates access control readers and doors.
- Be on the look-out for strange or suspicious objects.
- Visitors loitering around or other irregularities.
- Entire building and parking areas.

c. Security personnel must also pay attention to defects that could endanger people such as loose floor blocks and tiles, loose electrical wires, open electrical substation

d. After the Security personnel have completed the patrol, it must be entered in the Occurrence Register, as well as all problems/irregularities encountered, **i.e. all in order is not accepted**

e. Security personnel are requested to be very precise and thorough when executing a patrol. Alertness is a requisite.

f. Security personnel movements must be purposeful and any irregularities must be reported to Supervisor and Security Manager.

g. All assets and classified information confiscated during the night shift patrol must be kept in the security control point; day shift personnel must notify the owners.

14. Conclusion

The creation and maintenance of a secure work environment is the responsibility of every employee and any person that is authorized to gain access to any ULM premises. Day to day monitoring, supervision and correction of deviations from set procedures will counter any threat to the delivery of services by ULM.