PHYSICAL SECURITYPOLICY

JULY 2021

Table of Contents

1. Definition

1.1 Access control

It is the process by which physical access to a particular area is controlled or restricted to unauthorized persons.

1.2 Security Alarms

A security alarm is a system designed to detect intrusion or unauthorized entry into a building or area.

1.3 Applicant

Any person whose security competency is being investigated.

1.4 Author

The official who compiles, generates or initiate a document.

1.5 Authorized officer

The security officer who is delegated by the Municipal manager.

1.6 Accounting Officer

The Municipal Manager

1.7 Biometric

The measurement and statistical analysis of people's physical and behavioral characteristics.

1.8 CCTV

Close Circuit Television

1.9 Classification

All official documents, matters and information requiring the application of security measures must be classified and treated as confidential.

1.10 Compromise

The unauthorized disclosure / exposure or loss of sensitive or classified information or exposure of sensitive operations, people or places whether by intension or through negligence.

1.11 Contractor

The person who on behalf of Steve Tshwete Local Municipality accepts overall responsibility for performing the work as contracted or undertaking to deliver goods, or services to the organization.

1.12 Control room

The control center where all security activities are coordinated.

1.13 Confidentiality

Frequent efforts shall, therefore be made to rise conscious levels amongst the staffon the importance of security and the strict execution of the security policy at all times.

1.14 Consistency

Uniformity in the application of rules pertaining to security and standardization indealing with investigation of security breaches.

1.15 Copying

Making of a copy of any document whether by copying it by hand, photographic means, or by any other means.

1.16 Classified information

Sensitive information which the Municipal interest is under the control of the Municipality and which by the nature of its sensitivity must enjoy protection against compromise.

1.17 Declaration of secrecy

An undertaking given by a person who has or has had access to classifiedinformation, that he / she treat such information as secret.

1.18 Delegation

The transfer of authority, power or functions from one official to another. A delegate is an official who is granted certain powers and authority in order to represent another official in performing specific tasks.

1.19 Destruction of classified material

The doing away with or destroying of classified documents.

1.20 Industrial espionage

An attempt to obtain information through theft.

1.21 Information security

The condition created by the conscious provision and application of the document, personnel, physical, computer and communication security measures to protectsensitive/ classified information.

1.22 Investigation

The systematic search for the truth and gathering of valuable facts and or information regarding an incident.

1.23 Key Holder

Any person who is appointed by the Head of department to be in charge of keys.

1.24 MISS

Minimum Information Security Standards.

1.25 NIA

National Intelligence Agency.

1.26 Physical security

That condition created by the conscious provision and application of physical security measures for the protection of personnel, property, resources and information from harm or damage.

1.27 PSIRA

Private Security Industry Regulatory Authority.

1.28 Responsibility

All staff members are expected to play a role in ensuring that visitors or clients, personnel, assets and information of the Municipality is secured at all times. Staffmembers will not act in a way that will endanger the property, personnel and information.

1.29 Risk analysis

The identification and measurement of risks that endangers vulnerable assets ofan organization.

1.30 Risk Control Measures

It is principle that the Municipal Manager as the accounting officer of the Municipality is accountable for security. The Municipal Manager relies on Senior Manager Traffic & Security for the execution of the security policy and the implementation and maintenance of security measures in the Municipality.

1.31 Risk survey

The identification and measurement of current security weaknesses at a certain premise.

1.32 SANDF

South African National Defence Force.

1.33 SAPS

South African Police Services.

1.34 Search

To look through, to look at, to look at or beneath the superficial aspects of to discover a motive, reaction, feeling, basic truth; to go or look through (place, areaetc.) carefully in order to find something missing or lost; to look at or to examine(a person or object etc.) carefully in order to find something concealed.

1.35 Security

A process that entails the implementation or cost-effective security measures that,when taken as a whole, have the effect of reducing the probability of loss-incurringevents and reducing the impact of any loss-incurring events that might occur.

1.36 Security breach

To compromise security risk control measures.

1.37 Security measures

All actions, measures and means employed to achieve and ensure a condition ofsafety against any prevailing threats.

1.38 Security Officer

A private person who is paid to protect organization's assets from varioushazards by utilizing preventative measures.

1.39 Security vetting

The screening of an applicant.

1.40 Storage

The safe keeping of classified documents in appropriate lockable containers, strong rooms, record rooms and safes.

1.41 STLM

Steve Tshwete Local Municipality.

1.42 VIP

Very Important Person

1.43 HOD

Head of Department

2. Background

The Steve Tshwete Local Municipality is faced with the following challenges:

2.1 Theft of copper cables.

2.2 Theft of the Council's assets.

2.3 Vandalism of Council buildings.

2.4 Theft of information.

2.5 Theft of personnel's personal belongings.

2.6 Attack and intimidation of personnel while they are on duty.

3. Legal framework

3.1 Criminal Procedure Act 51 of 1977

3.2 Control of Access to Public Premises and Vehicles Act 53 of 1985

3.3 Trespass Act 6 of 1959

3.4 PSIRA Act 56 of 2001

3.5 Firearms Control Act 60 of 2000

4. Purpose

The purpose of the policy is to enforce access control and physical security at Steve Tshwete Local Municipality premises. The Security Policy is very effective and cheapest means of protecting property, personnel, and information against threats.

5. Objectives of the policy

5.1 To provide a safe, secure work environment and to minimize crime related lossesthat impact negatively on the organization.

5.2 To minimize losses resulting from theft and unauthorized access.

5.3 To prevent unauthorized access to the council's premises.

5.4 To prevent any form of industrial espionage.

5.5 To protect property, personnel and information against threats.

6. The Legal Mandate: Control of Access to Public Premises and Vehicles Act 53 of1985.

6.1 Section 2 (1) of the Act states that notwithstanding any rights or obligations to thecontrary and irrespective of how those rights or obligations arose or were grantedor imposed, the owner of any public premise or any public vehicle may

6.1.1 Take such steps as he/she may consider necessary for the safeguarding ofthose premises or that vehicle and the contents as well as for the protectionof the people therein or thereon.

6.1.2 Direct that those premises or that vehicle may only be entered upon in accordance with the provision of subsection (2).

6.1.3 Section 2 (2) of the Act states that no person shall without the permission of the authorized officer enter the public premises or any public vehicle in respect of which a direction has been issued under subsection (1) (b) and for the purpose of granting that permission officer may require of the person concerned that he/she.

6.1.4 Furnish his /her name, address and any other relevant information requiredby the Authorized officer.

6.1.5 Produce proof to the satisfaction of the Authorized officer.

6.1.6 Declare whether he/she has any dangerous object and or hazardous materials in his or her possession or custody or under his control; thereaftersecurity will liaise with the Occupational Health and Safety officer.

6.1.7 Declare what the contents are of any vehicle, suit case, bag, hand bag, folder, envelope, parcel or container of any nature which he/she has in hisor her possession or custody or under his or her control, and show those contents to him.

6.1.8 Subject him or her and anything which he/she have in his/her possession or custody or under his/ her control for examination or custody until he/sheleaves the premises or vehicle.

6.1.9 Hand to an Authorized Officer anything which he/she has in his possession or custody or under his control for examination or custody until he/she leaves the premises or vehicle.

7. Access control cards / Biometric systems

7.1 The access control card shall be issued by the Security Office, after the completion and approval of the access control card application form.

7.2 The individual access control card/tag holders are responsible and accountable for their cards and how they are used.

7.3 The access control card will be time specific, allowing the employee access to the council premises only during hours of duty.(from 07:00 to 17:00) Employees who work overtime time and stand by duties will access the premises accordingly provided their immediate supervisor has made arrangements.

7.4 Where access is gained through biometric systems, employees using the system shall have their finger prints captured into the access control data base.

7.5 Employees who breach access control procedures by leaving the doors open when they must be closed will be subjected to disciplinary procedures.

8. Application for access to particular areas

8.1 The Access / exit shall only be approved on the strength of an application formthat has been signed by the applicant and then approved by his or her manager.

8.2 Application forms for access control can be obtained from the security office.

8.3 The details of the employee will be captured into the access control data basesystem.

9. Recovery of Access cards

9.1 The Human Resources Department shall recover the card from the employee whose employment with the Steve Tshwete Local Municipality has been terminated and submit it to security services. The exit forms shall be circulatedto the Security so that the access card can be withdrawn and deactivated.

9.2 Employees who have resigned will be deactivated from the access control database system.

10. Lost access control cards

10.1 When the access control card is lost, the card holder must report the loss

tothe Security Office immediately or within 24 hours.

10.2 Damaged access cards will be returned to the Security office before areplacement card is issued.

10.3 An amount of R50.00 will be charged for access cards or access tags that have been lost.

11. Access Control Procedures at all Council building entrances for VIPs,employees, contractors, visitors and public members.

11.1 VIPs, employees, contractors, visitors and public members will give consent tobe searched by security officers. Any employee, visitor, contractor and or publicmember who does not consent to the searches by the security officers will be denied access/exit for security reasons. Employees shall were their name tags for easy identification at access control points.

11.2 Access arrangements for VIPs will be arranged with the security department bythe responsible department. VIPs and their body guards will not be subjected to searches at the entrance or exit points.

11.3 Employees, contractors, visitors, and public members entering the premises will be screened by means of a metal detector. All bags and parcels will be examined for any dangerous weapons such as knives, fire arms, screw drivers,Knobkerries and any sharp objects.

11.4 Removal of Council assets from one building to another will be carried out by means of a transfer form signed by one of the HOD or delegated person.

11.5 Any employee, contractor, visitor or public member will be required to declare any goods at the access control point. Details of the goods e.g. Laptop and those of the owner will be recorded. One will need to sign out when leaving thebuilding with goods where such access control measures exist.

11.6 All searches will be conducted with strict regard of the law, decency and orderwill be observed by Security Officers.

11.7 Without prejudice to the provisions of the Trespass act, 1959(Act 6 of 1959) anauthorized officer may at any time remove any person from any public premises or public vehicle if:

11.7.1 That person enters or enters upon the premises or vehicles concernedwithout the necessary permission.

11.7.2 The authorized officer considers it necessary for the safe guarding of the premises or vehicle concerned or the contents or for the

protectionof the people therein or thereon.

11.7.3 On all access control points, all employees, public members, contractors and visitors may be searched by the security officer. Whereone has signed in upon enteringthey must also sing out upon exiting.

11.8 Access to the premises by service providers contracted with the Municipality should be arranged by the relevant Department in conjunction with security office.

11.9 In an emergency situation the standby security should be notified.

11.10 Where identity scanners are provided at any access control point, employees, visitors and contractors will allow security officers to scan their ID documents, driver's license and or vehicle disk. Security officers will deny access/exit to any person who fails to comply with access control requirements. Disciplinary action will be taken against any person breaches any security risk control measures.

12. Office Security

12.1 Each employee is responsible for his or her own office security set out in the obligations and duties listed below as well stipulated elsewhere in this policy. Employees are responsible for closing windows when knocking off duty, lockingdoors and unlocking as required. The assets inside the office remains the responsibility of the employee to look after them and how they are used.

12.2 Employees are required to report unlockable doors, storage facilities and cabinets that require locking for purposes of safeguarding municipal assets and confidential or classified information, whether due to faulty mechanisms, damage or otherwise, to the Deputy Director: Traffic & Security and Assistant Director: Building Services immediately upon gaining knowledge thereof.

12.3 Employees are required to keep their offices locked when they are notattended.

12.4 At the end of the day, each employee should make sure that doors, windowsand cabinets are closed and locked.

12.5 Sensitive documents should be locked away to prevent theft of information.

12.6 The jamming of doors that are fitted with access control systems is strictlyprohibited.

12.7 Office hours for the purpose of access control are from 07: 00 to 17:00.

12.8 Security officers will be required to record details of any employees who enter the premises after normal working hours in the afterhours register. This applieson weekends and public holidays as well.

12.9 The Council Chamber and all boardrooms must be locked at all times whennot in use to prevent planting of bugging devices.

13. Key control

13.1 The relevant heads of departments will appoint officials who will beresponsible for the keys.

13.2 The heads of departments will submit a list of key holders to the Security Office. Contact details of the key holder must be furnished. (Office telephone and cell phone number).

13.3 Lost keys must be reported by the key holder to the Security Office and SAPSas soon as possible.

13.4 If the key holder resigns, keys must be returned to the head of departmentand if the security detects threat or any security breaches or risk it is advisable that the locks should be changed.

13.5 Duplication of keys without authorization is prohibited; any contravention ofthis rule will lead to disciplinary action.

13.6 A key control register must be implemented by all Departments. This is to ensure a proper handing over and receiving over, and maintain the record andmovement of keys.

14. Security Alarms

14.1 Security shall be responsible for installation, testing andmaintenance of security alarm systems.

14.2 Heads of departments will appoint the responsible person for access toarmed security alarm systems.

14.3 Sharing of security alarm codes is prohibited and should be reported as soonas possible.

14.4 Security alarms must be tested by the responsible person at least once amonth.

14.5 Faulty security alarms should be reported to the Security Office as soon aspossible.

14.6 Burglaries and other crimes must be reported to the Security Office, Executive Director: Finance and SAPS as soon as they have been discovered.

14.7 All new security alarm installations will be approved and supervised by thesecurity department.

14.8 The Security Services standby numbers will be published on the SteveTshwete Local Municipality website.

14.9 If the key holder discovers that the alarm system is faulty, he shall attempt to bypass the faulty zones. If the alarm is not armed the key holder will not leave the site. He or she will call the security personnel on standby to attend to the situation. A standby technician will be called in so that the problem can be resolved. The security stand by personnel will post a security officer if there is a need.

Procedures to be followed during alarm activation

14.10 The contracted armed response company receives the alarm activationsignal from the Council premises to their Control Room

14.11 The Control Room attendant calls the key holder or person in charge on the premise telephone line and confirms the situation during normal working hours. If there is no response, the control room attendant will call the key holder on his/her cell phone number. If the key holder is not available, the control room attendant will dispatch an armed reaction officer to go and investigate the cause of the alarm activation.

14.12 If there is a positive burglary, attempted burglary or armed robbery, the control room attendant will immediately call the Security Stand by number provided. The security stand by personnel will respond to the incident.

14.13 The key holder will report the incident to the nearest SAPS and the security department.

14.14 If a panic signal is received, the control room attendant will immediately send an armed reaction officer to investigate, if there was any armed robbery, burglary or any incident, the control room attendant will call the security stand by number.

14.15 All security irregularities must be reported to the security office immediately telephonically and then followed by a written incident report.

14.16 If the key holder discovers that the alarm system is faulty, he shall attempt to bypass the faulty zones. If the alarm is not armed the key holder will not

leave the site. He or she will call the security personnel on standby to attend to the situation. A standby technician will be called in so that the problem can be resolved. The security stand by personnel will post a security officer if there is a need.

15. Procedures for digital security systems (integrated security systems)

15.1 Employees wishing to gain access to such premises will make sure that, theimmediate supervisor has given them authorization.

15.2 The employee will contact responsible offsite monitoring control room todeactivate the system.

15.3 When the employee has finished his work he or she shall inform the controlroom to arm the system.

15.4 Control room contact details are displayed at the respective gates.

16. CCTV systems

16.1 The CCTV system will be linked to the 24 hour monitoring room. All CCTV recordings will be kept for a period of between 30 to 90 days and managed bythe security Office.

16.2 Only authorized personnel will be allowed to operate the CCTV system for security reasons. Only authorized staff members will be allowed access to theCCTV monitoring centre for the purpose of executing their official duties.

16.3 The recorded video footage shall be made available to the heads ofdepartments on request.

16.4 Responsible managers will on a monthly basis submit a report to the securitydepartment about the incidents that were observed.

16.5 All irregularities will be reported to the Deputy Director Traffic, Licensing andSecurity Services.

16.6 Viewing by public members is not allowed, unless the contrary is approved bythe Municipal Manager in writing.

16.7 Viewing by council personnel shall be allowed after a written request has been submitted to the security department.

17. Control of fire arms

17.1. Fire arms are not allowed at Steve Tshwete Local Municipality premises. Employees, visitors and contractors in possession of fire arms must leave their fire arms at the lockable gun safes at the security desk where ever access control is conducted.

.

17.2. The owner of the gun will be required to produce a license or permit for such a fire arm for the purpose of verification by the Security Officer. The owner of the gun will deposit his/her gun in the gun safe and take the key with him/her.

17.3. The SAPS members, Traffic Officers, Squatter Control Officers, SANDF members, In-house security officers and VIP protection units will not be required to leave their guns at the security desk when they are on official duty. They will complete the fire arms register and produce the fire arm license or permit if requested to do so by the Security Officer.

18. Guarding of premises (ADHOC)

18.1 The Steve Tshwete Local Municipality will deploy Security Officer at its premises to protects assets and enforce access control procedures.

18.2 Employees & contractors who breach security procedures will be subjected to disciplinary procedures.

18.3 Heads of departments will request security guards by making a written request to the Executive Director: Community Services.

18.4 If security officers are required for emergency purposes, a telephonic arrangement will be made with the Deputy Director of Traffic, and Security Services or Superintendent Security officer or delegated person. A written request will however be forwarded to the Deputy Director of Traffic, and Security Services as soon as possible. (About 24 hrs from the time of request ADHOC)

19. Procedures to be followed after an incident has occurred.

19.1 Immediately report the incident to the security department.

19.2 Incident that has the elements of crime must be reported to the nearest SAPS within 24 hours.

19.3 An incident report must be submitted to the security department within 48 hours.

19.4 The incident report must detail the following:

19.4.1 Introduction

19.4.1.1. The introduction must consist of the following:

19.4.1.2. Name and Surname of the person,

19.4.1.3. Identity number and designation of the person.

19.4.1.4. Address and contact details of the person,

19.4.1.5. Heading of the incident (Theft, Burglary etc.)

19.4.1.6. Date and time of the incident

19.4.1.7. Location or address of the incident

19.4.1.8. The incident should answer the following questions: (WHAT, WHERE, WHEN, HOW, WHO AND WHY)

19.4.1.9. Indicate the estimated value of the damage or loss.

19.4.1.10. Add attachments e.g. (pictures, receipts, etc.) where applicable.

19.4.1.11. The incident report must be signed before being submitted to the security department.

20. Security breaches

Any failure to adhere to the prescriptions of this policy constitutes a security breach and will lead to disciplinary procedures and or criminal action taken against any person.

21. Enforcement of this policy

21.1. Any crimes that are committed within the Council's premises will be reported to SAPS for investigation as soon as possible.

21.2. Any security breaches will lead to disciplinary action.

21.3. Employees, contractors are expected to report any security breaches that are observed.

22. Damage to council property.

22.1. The damage or accident should be reported immediately. If the incident happened during the presence of the security officers, details of the suspect will be taken down and the scene will be photographed as soon as possible.

22.2. During a vehicle accident all details will be taken down. Traffic officers will be called to attend to the scene.

22.3. The concerned department will submit a report to the security department within 48 hours. The security department will submit the report to the finance department.

22.4. The finance department will lay claims with the insurance service provider.

22.5. Whoever has caused damaged to the council property will be held liable by the insurance service provider.

22.6. Where the insurance claim becomes unsuccessful the finance department will

engage with the legal department to try and pursue the suspect and hold him/her accountable.

23. Responsibilities.

23.1. The Municipal Manager

Has the overall responsibility to manage the entire security risks within the Municipality.

23.2. The Executive Director Community Services

Will be responsible to enforce the security policy and monitor compliance and ensuring that all security related incidents are investigated and reported to the Municipal Manager.

23.3. Superintendent Security Services

Will be responsible for;

- The development of the security strategic plan and security policy and procedures.
- Taking a leading role in the implementation of the security strategic plan and policy and procedures and proposing amendments to the physical security policy and procedures for review and approval.
- Preparation and submission of security reports to the Executive Director Community Services.

23.4. Assistant Superintendents Security Services

They will be responsible for the day to day security operations and supervising the security officers.

23.5. Heads of Departments

Supported by the Security Services, they will be responsible for monitoring security related risks within their departments. They will also be responsible for ensuring that all security breaches and incidents within their departments are reported to the Superintendent Security Services.

23.6. Employees

All employees are expected to adhere to security control measures and report all security breaches and incidents to their supervisors and managers.

24. Security Risk Control Measures

All security measures that will be implemented by Steve Tshwete Local Municipality will conform or comply with the following:

- Private Security Regulatory Authority requirements.
- Best security practices; and liaison with all other relevant stakeholders.
- Other relevant council policies.

25. Implementation structures

25.1 Security steering committee

25.1.1 Composition

The Security Steering Committee shall be composed of members nominated and appointed from;

- Exco members
- Security Department
- Fire Department
- IT Services
- Building Services
- Finance Services

25.1.2 Appointment and tenure of office

The Security Steering Committee members shall be formally appointed by the MM for a period of 12 months.

25.1.3 Role and Responsibilities

The role and responsibilities of the Steering Committee shall include among others the following;

- Advising the Executive Management on all strategic security related matters.
- Ensuring that the Security Strategic plan is aligned with the wider Government directives, Policy priorities and STLM's IDP, objectives, Service delivery, Budget and Implementation Plan.
- Prioritizing the implementation of strategic projects in consultation with the Executive Management.
- Reviewing and recommending security projects to the MM for approval.
- Monitoring the implementation progress of security projects against budget, targets and deliverables.
- Reviewing and monitoring the performance of outsourced security service providers against signed SLAs.

25.1.4 Frequency of meeting

The Security Steering Committee shall meet quarterly and the minutes of meetings held and attendance registers shall be maintained.

25.2 Security Forum

The Security Forum shall be composed of the following;

- Exco members
- All Head of Departments

25.2.1 Role of the Security Forum

- To identify security issues or risks.
-
- To develop mitigation and contingency matters for the identified risks.
-
- To assist with budgeting of the mitigation matters.

25.2.2 Frequency of meetings for the Security Forum

They will meet twice a year or as and when required.

26. Applicability

The policy is applicable to,

26.1 All the departments and their related employees.

26.2 Contractors, Clients and Visitors at all Council facilities.

26.3 All government department doing business with the Municipality.

26.4 When applying the policy, consideration needs to be taken with regard to otherrelated legislation and policies e.g. Occupational Health and Safety; Risk Management, Disaster Management etc.

27. Review

The policy shall be reviewed annually and submitted to the council for approval.

28. Approval of the Policy

The table below shall be completed upon the approval of the policy by the council.

Document Title	Physical Security Policy and Procedures
Document Version	Version 1 of 2021
Compiled By	Superintendent Security Services
Recommended By	Executive Director Community Services
Approved By	Council Resolution(Insert Resolution No)
Date approved	To insert date

NB: ▶ **SECURITY IS EVERYBODY'S RESPONSIBILITY!!!**

▶ **SECURITY IS EVERYBODY'S BUSINESS!!!**