SA39/2005

SECURITY VETTING POLICY FOR MATJHABENG MUNICIPALITY (PS&T) (20/2)3

## PURPOSE OF REPORT

*** The purpose of the report is to seek approval from Council for the endorsement of the Security Vetting Policy for Matjhabeng Municipality.(See **Separate Cover)**

## INTRODUCTION AND BACKGROUND

The information, personnel, infrastructure and equipment are critically important assets of any institution. The integrity of these resources is however constantly threatened by organisations and individuals who conduct or plan devious activities e.g. sabotage, theft, subversions, etc. For the perpetrators of these devious activities their successful conduct is largely dependent on the ability to identify and exploit security related shortcomings within the institution (Matjhabeng). Vetting is thus a security measure that would be applied to members of Matjhabeng against undermining influences.

Security vetting is meant to establish as far as is reasonably possible, the security competence of the individual i.e. his/her integrity and reliability regarding the handling of classified information to which he/she is entitled to have access, by virtue of the post that he/she occupies. Security vetting is thus of the utmost importance to the security of Matjhabeng Municipality.

The outside legal opinion was seek by the Municipal Manager in an endeavour to establish any inherent infringement that might be propagated by the policy. The legal firm re-drafted the policy so as to be consistent with the Constitution and other pieces of legislations. The item that is being presented is the product of the legal opinion sought from external agencies.

## PROBLEM STATEMENT

None.

## POLICY POSITION

Resolution MC 255 - 22 August 2001 laid the basis for the development of this policy.

## RECOMMENDATIONS

1. That the Vetting Policy be approved as a form of personnel security in Matjhabeng.

2. That all employees of Matjhabeng be subjected to provisions of sections 3 and 4 of the Protected Disclosure Act 84 of 1982.

GOVERNANCE AND ADMINISTRATION CLUSTER RESOLVED : (31 AUGUST 2005)

1. That the Vetting Policy **BE APPROVED** as a form of Personnel Security in Matjhabeng.

2. That all employees of Matjhabeng **BE SUBJECTED** to provisions of Sections 3 and 4 of the Protected Disclosure Act 84 of 1982.

3. That the Acting Municipal Manager **SHOULD** identify crucial posts that has to go through the process of vetting and that **MUST** be in line with the Resolution MC255 – 22 August 2001

**IT WAS RESOLVED BY THE MAYORAL COMMITTEE TO RECOMMEND (19 OCTOBER 2005)**

1. That the Vetting Policy **BE APPROVED** as a form of Personnel Security in Matjhabeng.

2. That all employees of Matjhabeng **BE SUBJECTED** to provisions of Sections 3 and 4 of the Protected Disclosure Act 84 of 1982.

3. That the Acting Municipal Manager **SHOULD IDENTIFY** crucial posts that have to go through the process of vetting and that must be in line with the Resolution MC255 – 22 August 2001.

**SUBMITTED FOR CONSIDERATION.**

**SA39/2005**

**SECURITY VETTING POLICY FOR MATJHABENG MUNICIPALITY (PS&T)**
**(20/2) (P12 : SEPARATE COVER)**

**PURPOSE OF REPORT**

The purpose of the report is to seek approval from Council for the endorsement of the Security Vetting Policy for Matjhabeng Municipality.

**COUNCIL RESOLVED (1 NOVEMBER 2005)**

[AMPS&T] 1. That the Vetting Policy **BE APPROVED** as a working document as a form of Personnel Security in Matjhabeng.

2. That all employees of Matjhabeng **BE SUBJECTED** to provisions of Sections 3 and 4 of the Protected Disclosure Act 84 of 1982.

[AMM] 3. That the Acting Municipal Manager **SHOULD IDENTIFY** crucial posts that have to go through the process of vetting and that must be in line with the Resolution MC255 – 22 August 2001.

**(DA Cllr JJ Olivier indicated that schedule 1 and 2 of the Councillors and employees Code of Conduct must be included in the final document).**

**SEPARATE COVER**

**SA39/2005**

# SECURITY VETTING POLICY FOR MATJHABENG MUNICIPALITY (PS&T) (20/2)

# SECURITY VETTING POLICY FOR MATJHABENG MUNICIPALITY:

Reference:

A. Minimum information Security Standards (MISS) Cabinet Memorandum No 4 of 1996).

B. National Personnel Security Vetting Policy Guidelines.

C. National Strategic Intelligence Act, 1994 (Act No 39 of 1994)

D. Promotion of Access to information Act, 2000 (Act No 2 of 2000)

E. Protection of information Act 84 of 1982

## INTRODUCTION

Every institution, state or private, has something unique that needs to be protected from being divulged in an untimely and unauthorised fashion. Matjhabeng, like any other institution of state, has a statutory obligation to protect its assets, information and personnel against any immediate, latent or potential threat by hostile organisations (undesirable or criminal elements).

Employees/personnel are always at the receiving end as they are constantly exposed their of susceptible to manipulations or/and any other form of pressure to fulfil the aspirations of their adversaries. Due to these overly pressures and other socio economic factors employees commit or fail to report acts of corruption, bribery, extortion, blackmail, fraud, sabotage, espionage, etc to the relevant authorities.

Much of the institutions like Matjhabeng security depend entirely on the integrity and reliability of its employees and contractors with regard to the handling of "classified information". Security vetting, as a means to safeguard employees and their vital interests, is of the utmost importance to the security of the municipality. For this reason security vetting must be done in respect of all personnel who have access to classified information. **Please note:** Information about municipal infrastructures, e.g. dams, telecommunication networks, firewalls, buildings, tender or proposal documents, etc is vita to criminals and other hostile organisations and there is therefore a need to classify them.

Security vetting is a means to establish as far as is reasonable possible, the security competence of the individual i.e. his/her integrity and reliability regarding the handling of classified information to which he/she is entitled to have access to, by virtue of the post that he/she occupies. Security vetting is thus of the utmost importance to the security of Matjhabeng Municipality.

## AIM

The aim of this document is to provide a policy framework with reference to the security vetting process, to which all members and/or employees of Matjhabeng Local Municipality and any person who requires access to classified Council information and premises shall be subjected.

## SCOPE

This document outlines the scope of the policy to be followed by Matjhabeng when doing security vetting and is structured as follows:

**Definitions:**

Legal mandate.
Maintenance of security within the Matjhabeng Local Municipality.
Factors influencing Security Competence.
Categories of persons to be subjected to the security vetting process.
Management responsibility regarding security vetting.
Validity period of security clearances.
Application procedures.
Vetting process.

## DEFINITIONS

The following definitions apply:

"**Applicant**" means any employee of person whose security competence is being investigated, including person(s) to be appointed as employee(s).

"**Classified information**" means sensitive information which is in the national interest of and is under the control of the **municipality**, or which concerns the municipality and which by reason of its sensitive nature must be exempted from disclosure and must enjoy protection against compromise. Such information would be classified as either **CONFIDENTIAL OR SECRET** according to the degree of damage the municipality may suffer as a consequence of is unauthorised disclosure.

"**Compromise**" means that the particulars of classified information/matters became known to unauthorised person(s).

"**Employee**" means any person appointed as such by the Municipality in terms of applicable legislations.

"**Member**" means, in relation to this policy, any Councillor or any employee occupying any position within the municipality.

"**need-to-know principle**" means no person is entitled to obtain access to classified information solely by virtue of positions, appointment or security clearance. Access is to be restricted to that information or par thereof which is essential to the execution of the person's official duties, that is, on a need-to-know basis.

"**Personnel security**" means the protection of personnel against subversion, undue influence, bribery, blackmail, intimidation and other criminal activities.

"**Physical security**" means the set of measures implemented and/or applied to ensure the safeguarding of all classified information, personnel facilities or material. It includes physical barriers such as perimeter protection alarm systems, locks, keys and safes.

"**Security clearance**" means a written declaration by the Municipal Manager that a person is eligible under the standards of this policy to access information with a specified grade/level of security classification, which is necessary for the execution of his/her official duties.

"**Security competence**" means a person's integrity and reliability regarding the handling of classified information and includes factors such as his/her vulnerability to extortion, blackmail and bribery as well as negligence in the handling of classified information and includes the ability to act in such a manner that he/she does not bring about the disclosure of classified information or

material (in written or oral form) to an unauthorised person and in this way endanger the security interests of the institution.

"Security vetting" means a systematic investigative process to determine a person's security competence by having regard to any information, including private information, at the disposal of the municipality, provided that such information need not be confined to information that will be accessible to the person in the normal course of his/her duties.

"Security risk" means a person is a security risk when he/she, because of personality traits, needs, behaviour, ideological persuasion or extreme sensitiveness in respect of past deeds, can be persuaded by whatever means to co-operate with an unauthorized individual/organisation to divulge secret or confidential information of his/her employer or of his/her own accord divulges secret or confidential information to an unauthorised individual/organisation.

## LEGAL MANDATE

The vetting mandate is directly and indirectly derived from the enactments listed below.

## NATIONAL STRATREGIC INTELLIGENCE ACT, 1994 (ACT 39 OF 1994)

In terms of section 2 of the National Strategic Intelligence Act, 1994 (Act 39 of 1994) the National Intelligence Agency (NIA) has the national counter-intelligence responsibility, which includes steps and measures to neutralise foreign or hostile intelligence operations and to protect classified information. The South African Intelligence Organisations and the SAPS are the only institutions in terms of this Act, mandated to conduct vetting.

## PUBLIC SERVICE ACT, 1994 (R103 OF 1994)

The Public Service Act (1994 R 103 of 1994) contains various references to vetting-related matters. In terms of section 3(4)(c) thereof the Public Service Commission may issue mandates regarding security requirements with which officers and employees shall comply.

In terms of section 17(2)(h) thereof the Public Service Commission may be discharged if his/her continued employment constitutes a security risk for the State. Some forms of misconduct as defined in section 20 of that Act may in certain circumstances also be of security importance and, therefore, become the subject of a vetting investigation.

## SCHEDULE 1, SECTION 10(1) TO (3) OF THE LOCAL GOVERNMENT SYSTEMS ACT 32 OF 2000

## THE PROTECTION OF INFORMATION ACT 84 OF 1982

Section 3 and 4 of the Act.

## MAINTANANCE OF SECURITY WITHIN THE MATJHABENG LOCAL MUNICIPALITY

Every member and/or employee of Matjhabeng Local Municipality will at all times be responsible and accountable for the maintenance of the security of information, personnel and material within his/her area of responsibility.

All information produced by or for, held by or for, or controlled by Matjhabeng Local Municipality, the disclosure of which to an unauthorised organisation, institution or person may harm the municipality security interests, is to be graded by means of a security classification and protected accordingly.

Each post within Matjhabeng Local Municipality is to have a security grading in accordance with the security classification of the information to which it is exposed.

All employees identified in accordance with the recruitment and selection policy and members, are to possess a security clearance, issued by the National Intelligence Agency, in accordance with the security classification of the information to which the member and/or employee requires access in order to perform his/her official duties.

No person is entitled to obtain access to classified information solely by virtue of position, appointment or security clearance. In all cases, access is to be restricted to that information or part thereof that is essential to the performance of the person's official duties, i.e. on a need-to-know basis.

## FACTORS INFLUENCING SECURTIY COMPETENCE

The fundamental rights enshrined in the Constitution will be the point of departure in every investigation. In assessing an applicant's security competence, the following will be considered:

**Value system:** An applicant's membership of a body, his/her views and/or beliefs and his/her morals, principles, which may at present, or in the future, endanger the security of the State, must be thoroughly investigated. While extreme beliefs, and how those influence the behaviour profile regarding the applicant's security competence, must be noted.

**Criminal and Departmental offences:** All criminal and Departmental offences must be taken into consideration. In this regard any act or omission punishable upon conviction in judicial proceedings (departmental or national) is considered.

**Behaviour and Personal Conduct Endangering Security (Acts or Omissions Endangering Security).** Behaviour endangering security refers to any conscious or unconscious acts/behaviour or negligence that exposes the Municipality's classified information, personnel, facilities or material to any exploitation that may be detrimental to the security of the Municipality. Conscious or unconscious non-compliance with security regulations and other behaviour endangering security raise doubts about an individual's trustworthiness, willingness and ability to safeguard classified information. This includes refusal to undergo or co-operate with required security forms and releases, or provide full, frank and truthful answers to lawful questions of investigators, vetting officers or other official representatives in terms of security vetting determinations. This also includes any conduct involving questionable judgement, untrustworthiness, unreliability, lack of candour and dishonesty.

**Use of Addictive Substances:** Addiction usually has a negative influence on a person's financial situation; his/her work performance and health. Such a person may become a security risk as addiction often leads to questionable judgement, unreliability, failure to control impulses and impairment of social functioning as well as increasing the risk of unauthorised disclosure of classified information as result of negligence and vulnerability to being manipulated, bribed, exploited or blackmailed.

**Financial status:** When a person has financial problems this may have serious implications for his/her security competence and must be investigated. When a person's lifestyle indicates an unexplained source of income (i.e. sudden affluence) it should be investigated.

**Misuse of information Technology Systems:** Failure to comply with rules, procedures, guidelines or regulations, pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness and ability to protect classified systems, networks and information properly. Information technology systems include all related equipment used for the

communication, transmission, processing, manipulation and storage of classified or sensitive information.

## CATEGORIES OF PERSONS TO BE SUBJECTED TO THE SECURITY VETTING PROCESS

### Persons with Access to Confidential information

A Confidential clearance must be issued to a member and/or employee before he/she is allowed access to information of a confidential nature. Persons recruited for specific posts for which a Confidential (or higher level) clearance is required must be issued with the required level of clearance before he/she is appointed in the post of allowed access to information requiring the relevant clearance.

**Persons with Access to Secret Information:** A secret clearance must be issued to a member and/or an employee before he/she is allowed access to information of a secret nature. This would include all managers from level 0-3. NB: Policy on recruitment and selection of the Matjhabeng Municipality contains all the necessary levels.

**Persons with Access to Top Secret information:** A Top Secret clearance must be issued to a member and/or an employee before he/she is allowed access to information of a top secret nature. This would include inter alia, the Municipal Manager, IT Manager and any other member exposed to sensitive information, investigators, EM PS & T etc.

### Appointment

Advertisements for vacant posts in Matjhabeng should state that the appointment of any member and/or employee in the Municipality is subject to person obtaining the appropriated grade of security clearance that the post requires. All appointments shall be provisional pending the issuing of a security clearance. While he/she is on probation, the services of any new employee who does not qualify for the grade of security clearance the post requires will terminated and such a person will not be permanently appointed in Matjhabeng Municipality. Any new employee, after he/she has been selected/recommended by the interview panel, must undertake in writing to resign from the Council, after following due process, should National Intelligence Agency refuse his/her application for a security clearance.

Security clearance is not coupled to position but to access information the post provides. Therefore, the security clearance requirements regarding the promotion/appointment of any member and/or employee will be determined by the security grading of the post occupied/to be occupied.

All members and/or employees should be issued with required security clearance prior to being appointed into another post.

### Persons working on Municipal IT Systems

Personnel working on municipal IT systems require a security clearance in accordance with their level of access.
The minimum security clearance requirement for all ICT computer system managers is a Top Secret clearance due to the nature of information they handle on a daily basis.

**Persons without Valid Identity Documents:** No security clearance can be issued to any person who is not in possession of a valid RSA identity document. Temporary identification documents are not acceptable for security vetting purpose.

## MANAGEMENT RESPONSIBILITY REGARDING SECURITY VETTING

Managers at all levels shall ensure that their subordinates are in possession of a valid security clearance issued by National Intelligence Agency.

Managers shall ensure that the level of security clearance required by a subordinate, member and/or employee or contractor corresponds with the security classification of the information to which the person requires access, in order to execute his/her official duties. To achieve this, managers at all levels shall ensure that every post in their area of responsibility is graded according to the security classification of the information to which the appointed person is exposed.

Security Risks: should it come to the attention of a manager that the action, omissions/negligence or circumstances of a member and/or employee under his management pose a risk to security, the manager must reconsider the relevant member's and/or employee's access privileges in accordance with the gravity of the actions, omissions, negligence or circumstances concerned. The access privileges can only be terminated after a thorough investigation has confirmed the existence of a security risk.

Expired security clearance: Managers may allow a member and/or employee of the municipality whose security clearance has expired and whose application for the renewal of his/her security clearance has already been received by NIA access to information classified up to the same level of his/ her expired security clearance.

## REPORTING OF ASPECTS INFLUENCING THE SECURITY COMPETENCE OF A MEMBER AND/OR EMPLOYEE OF MATJHABENG MUNICIPALITY

Managers at all levels shall ensure that all aspects or incidents which may influence a person's security competence are reported to security, via existing channels regardless of the security clearance of the person involved.

The following aspects shall be reported:

Any actions, negligence or behaviour which exposes the Municipal's classified information, personnel, facilities or material to any exploitation which may be detrimental to the security of the Municipality.

Any belief, philosophy, creed, opinion, and/or conviction which impairs or endangers another person's life, dignity, freedom, security of equality before the law and/or which impairs or endangers the security of the Municipality.

Extreme behaviour in the form of radical acts, acts of violence or terror, murder, intimidation or intimidating behaviour.

Addiction two alcohols, drugs, medicine or other addictive substances (excluding tobacco) indicative of a continued pattern of usage.

Repeated lapses into financial difficulties that indicate a person's inability to manage his/her personal finances and/or illegal enrichment.

Obvious personality changes, due to brain damage, serious operations, etc a distinction must be made between relatively permanent changes and temporary stress factors that may influence the personality functions (such as marital problems, menopause, job dissatisfaction or grievances, etc.)

Treatment for psychological problems, psychiatric illness/behavioural disorders and social problems that might impair or endanger the security of the Municipality.

An in-depth investigation by NIA on request of the relevant manager, will determine whether the reported aspects/incidents will have any influence on the security competence of the member and/or employee.

## VALIDITY PERIOD OF SECURITY CLEARANCE

Managers at all levels must ensure that a person, in respect of whom a security clearance has been issued is re-vetted (subject to the condition that such a person still occupies a post regarding the same or higher level of security clearance as the expired clearance), on a year to year basis.

Once issued a security clearance can be subjected to review/revision by National Intelligence Agency at any time and if necessary, be withdrawn or altered by the Municipal Manger as the case may be. The rules of natural justice shall however be applied is such case.

**Maternity leave:** Any level of security clearance issued to female members and/or employees who go on maternity leave, remains valid on condition that the period of leave does not exceed twelve months, should a woman resign before the confinement, she retains her clearance on condition that the interruption of service does not exceed 90 days.

### Validity of Security Clearances Issued by other Government Departments

A security clearance issued in respect of a member and/or employee while he/she is attached to a particular government institution is not automatically transferable to the municipality e.g. when the member and/or employee is transferred or join the municipality from one State department.

When a person changes his/her employer, the new employer has the responsibility to decide whether his/her existing clearance will be accepted or whether his/her re-vetting will be required in the prescribed manner. In the case of a person from another institution applying for a post in Matjhabeng Municipality, the person's security vetting file will be re-valuated and a decision will be made on whether that person has to submit to re-vetting or not.

## APPLICATION PROCEDURES

All persons applying for the issuing, re-issuing or upgrading of a security clearance shall submit their applications (completed Z204) to the Department of Public Safety and Transport.

### Confidential clearance

An application for Confidential Clearance consists of the following documents to be forwarded to NIA:

- Z204 and fingerprints;
- Consent to SAPS Criminal Record Inquiry;
- A certified copy of the member's and/or employee's RSA identity document or passport;
- A covering letter form the Municipal Manager

**Other Grades of Security Clearance:** Persons applying for all other levels of security clearance must complete the Z204, including all appendices.

Applications for Confidential, Secret and Top Secret clearances shall be accompanied by a covering letter form the Municipal Manager. Further documents to be forwarded with the application by the member's and/or Municipal Manager include"

a) an extract of the member's and/or employee's conduct sheet,
b) A report on aspects that may influence the security competence of the member and/or employee, to be completed and signed by the member's and/or employee's manager.

**Fingerprints**

Each application for a security clearance must be accompanied by a new set of fingerprints. Fingerprints are to be taken only by the SAPS or other authorise persons. It is compulsory to complete "indemnity by applicant".
In order to prevent the compromise of information, the application must preferably be sealed by the security personnel officer before despatch.

Applications with negative recommendation and/or negative information must be sealed by the manager in person, before being despatched. A person, who does not comply with the minimum security standards, may not be employed by the Municipality.

**VETTING PROCESS**

**Polygraph and Psychometric Tests:**. The following general guidelines shall apply:

- All applicants for Top Secret Clearances will be subjected to psychometric and a polygraph test regardless of their specific postings.
- Applicants for any other grade of clearance will be subjected to psychometric and polygraph test as deemed necessary, depending on the nature of information obtained by other vetting actions.

The polygraph should be seen as an aid in the security vetting process, and cannot replace thorough investigation. If any applicant refuses to undergo a polygraph test, to have his/her fingerprints taken or to submit information/documentation, he/she shall be informed that a more in-depth (and possibly lengthier) investigation will have to be conducted, if a security vetting field worker is unable to make a recommendation as a result of lack of information, the applicant will once again be given the opportunity to give his/her voluntary co-operation.

**Continuous Vetting:**

A successful security clearance process does not end when an applicant is issued with a security clearance, but must continue with frequent and productive reinvestigations done by the Municipal Manager. There are certain situations and requirements that necessitate productive reinvestigations. There are certain situations and requirements that necessitate re-vetting. When a person's conduct is of such a nature that it might pose a threat to council security or the effective protection of information in the Council re-vetting must be done.

**Cancellation and Termination of Applications**

In case a security clearance in process is no longer required (because of transfers, resignations, retirements, deaths, etc) NIA will be informed accordingly in writing by the Municipal Manager.

M161/2003

SECURITY VETTING POLICY FOR MATJHABENG MUNICIPALITY (20/2)(PS&T)

PURPOSE OF REPORT

The purpose of the report is to inform the Management-, Section 80- and Mayoral Committee of the Security Vetting Policy for Matjhabeng Municipality.

INTRODUCTION AND BACKGROUND

The information, personnel, infrastructure and equipment are critically important assets of any Institution, including Matjhabeng. The integrity of these resources is however constantly threatened by organisations and individuals who conduct or plan devious activities e.g. sabotage, theft, sub-versions, etc. For the perpetrators of these devious activities the successful conduct is largely dependent on the ability to identify and exploit security related shortcomings within the Institution (Matjhabeng). Vetting is thus a security measure that would be applied to members of Matjhabeng against undermining influences.

Security vetting is meant to establish as far as is reasonably possible, the security competence of the individual i.e. his/her integrity and reliability regarding the handling of classified information to which he/she is entitled to have access, by virtue of the post that he/she occupies. Security vetting is thus of the utmost importance to the security of Matjhabeng Municipality.

*** The security vetting policy for Matjhabeng Municipality is herewith attached on pages 20 - 29 of the Annexures

PROBLEM STATEMENT

None.

POLICY POSITION

None.

COMMENT: OTHER HEADS OF DEPARTMENTS

The policy has already been served before the Municipal Manager and has in principle agreed with the contents thereof

SUBMITTED FOR CONSIDERATION.

M161/2003

**SECURITY VETTING POLICY FOR MATJHABENG MUNICIPALITY (20/2) (PS&T) (P 18 : ANNEXURES P 20-29)**

**THE MANAGEMENT COMMITTEE RESOLVED: (3 NOVEMBER 2003)**

That this item **BE REFERRED BACK** to the next Management meeting to seek legal opinion externally.

# SECURITY VETTING POLICY FOR MATJHABENG MUNICIPALITY

Reference A: Minimum Information Security Standards (MISS) (Cabinet Memorandum No 4 of 1996).

B: National Personnel Security Vetting Policy Guidelines. (Approved NICOC Co-ordinator 28 Jan 99)

C: National Strategic Intelligence Act, 1994 (Act 10 No 39 of 1994)

D: Promotion of Access to Information Act, 2000 (Act No 2 of 2000)

## INTRODUCTION

1. The Republic of South Africa (RSA), like any other state, has an obligation to make security arrangements for the protection of its citizens and its vital interests. The RSA as a member nation of international organisations and signatory to international agreements/protocols must comply with certain minimum requirements in this respect.

2. Much of the State's security depends on the integrity and reliability of its civil servants and contractors with regard to the handling of classified information. Security vetting, as a means to safeguard its citizens and vital interest, is of the utmost importance to the security of the State. For this reason security vetting must be done in respect of all personnel who have access to classified information.

3. Security vetting is meant to establish as far as is reasonably possible, the security competence of the individual i.e. his/her integrity and reliability regarding the handling of classified information to which he/she is entitled to have access, by virtue of the post that he/she occupies. Security vetting is thus of the utmost importance to the security of Matjhabeng Municipality.

## AIM

4. The aim of this document is to provide a policy framework wrt the security vetting process, to which all members and/or employees of Matjhabeng Local Municipality and any person who requires access to classified Council's information and premises must be subjected.

## SCOPE

5. This document outlines the scope of the policy to be followed by Matjhabeng when doing security vetting. The document will be structures as follows:

a. Definitions

b. Legal Mandate

c. Maintenance of security within the Matjhabeng Local Municipality

d. Factors influencing Security Competence

e. Categories of Persons to be subjected to the security vetting process.

f. Management responsibility regarding security vetting.

g. Reporting aspects influencing the security competence of a member and/or employee of the Matjhabeng Municipality.

h. Validity period of security clearances.

i. Application procedures.

j. Vetting process.

**DEFINITIONS**

5. The following definitions applies:

a. **"Applicant"** means any person whose security competence is being investigated including present and potential employees.

b. **"Classified information"** means sensitive information which, in the national interest or is under the control of the State, or which concerns the State and which must by reason of its sensitive nature be exempted from disclosure and must enjoy protection against compromise. Such information is classified as either **RESTRICTED, CONFIDENTIAL, SECRET** or **TOP SECRET** according to the degree of damage the State may suffer as a consequence of its unauthorised disclosure.

c. **"Compromise"** means that the particulars of classified information/matters become known to unauthorised person(s) or there is a strong possibility that such particulars have become known.

d. **"Employee"** means a person appointed by the Municipality in terms of the Public Service Act, 1994 and the Municipal Systems Act, 2000.

e. **"Member"** means, in relation to this policy, any Councillor or any employee of any other rank.

f. **"Need-to-know principle"** means no individual is entitled to obtain access to classified information solely by virtue of position, appointment or security clearance. Access is to be restricted to that information or part thereof which is essential to the execution of the person's official duties, that is, on a need-to-know basis.

g. **"Personnel Security"** means the protection of personnel against subversion, dangerous influences, bribery, blackmail, intimidation and other criminal activities.

h. "**Physical Security**" means the set of measures implemented and/or applied to ensure the safeguarding of all classified information, personnel, facilities or material. It includes physical barriers such as perimeter protection alarm systems locks, keys and safes etc.

i. **"Project Security"** means all the security actions and measures that are initiated and/or carried out to ensure that the necessary level of security is maintained throughout the life cycle of a project.

j. **"Security Clearance"** means a written declaration by an authorised official that a person is eligible under the standards of this policy to access information with a specified grade/level of security classification, which is necessary for the execution of his/her official duties. The HOD Public Safety and Transport is the delegated and authorised official.

k. "**Security Competence**" means a person's integrity and reliability regarding the handling of classified information and includes factors such as his/her vulnerability to extortion, blackmail and bribery as well as negligence in the handling of classified information. It is the ability of a person to act in such a manner that he/she does not bring about the disclosure of classified information or material (in written or oral form) to an unauthorised person and in this way endanger the security interests of the institution.

l. "**Security Vetting**" means a systematic investigative process to determine a person's security competence, and is one of the most basic defensive measures in the protection of classified information:

   i. Such information need not be State information as such, but could also be private information entrusted to the State.

   ii. Furthermore, such information need not be confined to information that will be accessible to the official in the normal course of his/her duties.

m. "**Security Risk**" means a person is a security risk when he/she, because of personality traits, needs, behaviour, ideological persuasion or extreme sensitiveness in respect of past deeds, can be persuaded by whatever means to co-operate with an unauthorised individual/organisation to divulge secret or confidential information of his/her employer or of his/her own accord divulges secret or confidential information to an unauthorised individual/organisation.

## LEGAL MANDATE

7. The vetting mandate is directly and indirectly derived from the enactments listed below.

## NATIONAL STRATREGIC INTELLIGENCE ACT, 1994 (ACT 39 OF 1994)

8. In terms of section 2(1)(b) of the National Strategic Intelligence Act, 1994 (Act 39 of 1994) the National Intelligence Agency (NIA) has the national counter-intelligence responsibility, which includes steps and measures to neutralise foreign or hostile intelligence operations and to protect classified information.

## PUBLIC SERVICE ACT, 1994 (R103 OF 1994)

9. The Public Service Act (1994 R 103 of 1994) contains various references to vetting-related matters. In terms of section 3(4)(c) the Public Service Commission may issue mandates regarding security requirements with which officers and employees shall comply.

10. In terms of section 17(2)(h) an employee may be discharged if his/her continued employment constitutes a security risk for the State. Some forms of misconduct as defined in section 20 of the Act may in certain circumstances also be of security importance and, therefore, become the subject of a vetting investigation.

## MAINTENANCE OF SECURITY WITHIN THE MATJHABENG LOCAL MUNICIPALITY

11. Every member and/or employee of Matjhabeng will at all times be deemed to be responsible and accountable for the maintenance of the security of information, personnel and material within his/her area of responsibility.

12. All information produced by or for, held by or for, or controlled by Matjhabeng, the disclosure of which to an unauthorised organisation, institution or person may harm national security interests, is to be graded by means of a security classification and protected accordingly.

13. Each post within Matjhabeng is to have a security grading in accordance with the security classification of the information to which the relevant post provided access.

14. All members identified in accordance with the recruitment and selection policy are to possess a security clearance, issued by the National Intelligence Agency, in accordance with the security classification of the information to which the member and/or employee requires access in order to perform his/her official duties.

15. No individual is entitled to obtain access to classified information solely by virtue of position, appointment or security clearance. In all cases, access is to be restricted to that information or part thereof that is essential to the performance of the person's official duties, i.e. on a need-to-know basis.

## FACTORS INFLUENCING SECURITY COMPETENCE

16. The fundamental rights enshrined in the Constitution will be the point of departure in every investigation. In assessing an applicant's security competence, the following will be considered:

a. Value System. An applicant's membership of a body, his/her views and/or beliefs, or his/her morals, principles, which may at present, or in future, endanger

the security of the State, must be thoroughly investigated. Furthermore, extreme beliefs, and how these influence the behaviour profile regarding the applicant's security competence, must be noted.

b. Criminal Offences. All criminal offences must be taken into consideration. In this regard any act or omission punishable upon conviction in judicial proceedings (departmental or national) is considered.

c. Behaviour and Personal Conduct Endangering Security (Acts or Omissions Endangering Security). Behaviour endangering security refers to any conscious or unconscious acts/behaviour or negligence that exposes the Council's classified information, personnel, facilities or materiel to any exploitation that may be detrimental to the security of the Council. Conscious or unconscious non-compliance with security regulations and other behaviour endangering security raise doubts about an individual's trustworthiness, willingness and ability to safeguard classified information. This includes refusal to undergo or co-operate with required security processing or refusal to complete required security forms and releases, or provide full, frank and truthful answers to lawful questions of investigators, vetting officers or other official representatives in terms of security vetting determinations. This also includes any conduct involving questionable judgement, untrustworthiness, unreliability, lack of candour and dishonesty.

d. Use of Addictive Substances. Addiction usually has a negative influence on a person's financial situation, his/her work performance and health. Such a person may become a security risk as addiction often leads to questionable judgement, unreliability, failure to control impulses and impairment of social functioning as well as increasing the risk of unauthorised disclosure of classified information as a result of negligence and vulnerability to being manipulated, bribed, exploited or blackmailed.

e. Financial Status. When a person has financial problems this may have serious implications for his/her security competence and must be investigated. When a person's lifestyle indicates an unexplained source of income (sudden affluence) it should be investigated.

f. Behavioural Disorders. Irrespective of the nature of any mental disorder or behavioural problems, it is important to obtain a general impression of a person's behaviour and personality traits.

g. Misuse of Information Technology Systems. Failure to comply with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness and ability to protect classified systems, networks and information properly. Information technology systems include all related equipment used for the communication, transmission, processing, manipulation and storage of classified or sensitive information.

## CATEGORIES OF PERSONS TO BE SUBJECTED TO THE SECURITY VETTING PROCESS

17. Persons with Access to Confidential Information.

a. A Confidential Clearance must be issued to a member and/or employee before he/she is allowed access to information of a confidential nature.

b. Persons recruited for specific posts for which a Confidential (or higher level) clearance is required must be issued with the required level of clearance before he/she is appointed in the post or allowed access to information requiring the relevant clearance.

18. Persons with Access to Secret Information. A Secret clearance must be issued to a member and/or employee before he/she is allowed access to information of a secret nature. This would include all managers from level 0 – 3. NB. Policy on recruitment and selection of the Matjhabeng Municipality contains all levels.

19. Persons with Access to Top Secret Information. A Top Secret clearance must be issued to a member and/or employee before he/she is allowed access to information of a top secret nature. This would include *inter alia*, IT department, investigators, etc.

20. Appointment

a. **Advertisements for vacant posts in Matjhabeng should state that the appointment of any member and/or employee in the Council is subject to the person obtaining the appropriate grade of security clearance that the post requires. An appointment in these posts will be provisional pending the issuing of a security clearance. While he/she is on probation, the services of any new applicant who does not qualify for the grade of security clearance the post requires will be terminated and such a person will not be permanently appointed in Matjhabeng. Any new applicant, after he/she has been selected/recommended by the interview panel, must undertake in writing to resign from the Council, after following due process, should National Intelligence Agency refuse his/her application for a security clearance.**

b. Security clearance is not coupled to position but to the access the post provides. Therefore, the security clearance requirements regarding the promotion/appointment of any member and/ or employee will be determined by the security grading of the post occupied/to be occupied.

c. All members and/or employees should be issued with the required security clearance prior to being appointed into another post.

21. Persons Working on Council IT Systems

a. Personnel working on Council IT systems require a security clearance in accordance with their level of access.

b. The minimum security clearance requirement for all mainframe computer system managers is a Secret clearance.

22. Persons without Valid Identity Documents. No security clearance can be issued to any person who is not in possession of a valid RSA identity document. Temporary identification documents are not valid for security vetting purposes.

## MANAGEMENT RESPONSIBILITY REGAQRDING SECURITY VETTING

23. Managers at all levels shall ensure that their subordinates are in possession of a valid security clearance issued by National Intelligence Agency.

24. Managers shall ensure that the level of security clearance required by a subordinate, member and/or employee or contractor corresponds with the security classification of the information to which the person requires access, in order to execute his/her official duties. To achieve this, managers at all levels shall ensure that every post in their area of responsibility is graded according to the security classification of the information to which the appointed person is exposed.

25. Security Risks. Should it come to the attention of a manager that the actions, omissions/negligence of circumstances of a member and/or employee under his management pose a risk to security, the manager must reconsider the relevant member's and/or employee's access privileges in accordance with the gravity of the actions, omissions, negligence or circumstances concerned. The access privileges can only be terminated after a thorough investigation has confirmed the existence of a security risk.

26. Expired Security Clearances. Managers may allow a member and/or employee of the Council whose security clearance has expired and whose application for the renewal of his/her security clearance has already been received by NIA access to information classified up to the same level of his/her expired security clearance.

## REPORTING OF ASPECTS INFLUENCING THE SECURITY COMPETENCE OF A MEMBER AND/OR EMPLOYEE OF MATJHABENG MUNICIPALITY

27. Managers at all levels shall ensure that all aspects or incidents which may influence a person's security competence are reported to HOD Public Safety and Transport, via existing channels regardless of the security clearance of the person involved.

28. The following aspects shall be reported:

a. Any actions, negligence or behaviour which exposes the Council's classified information, personnel, facilities or materiel to any exploitation which may be detrimental to the security of the Council.

b. Any belief, philosophy, creed, opinion, and/or conviction which impairs or endangers another person's life, dignity, freedom, security of equality before the law and/or which impairs or endangers the security of the Council.

c. Extreme behaviour in the form of radical acts, acts of violence or terror, murder, intimidation or intimidating behaviour.

d. Addiction to alcohol, drugs, medicine or other addictive substances (excluding tobacco) or the frequent use of drugs, medicine or other addictive substances (excluding tobacco), indicative of a continued pattern of usage.

e. Repeated lapses into financial difficulties that indicate a person's inability to manage his/her personal finances and/or illegal enrichment.

f. Obvious personality changes, due to brain damage, serious operations, etc. A distinction must be made between relatively permanent changes and temporary stress factors that may influence the personality functions (such as marital [problems, problems experienced in relationships, death of loved ones, financial problems, menopause, job dissatisfaction or grievances, etc.).

g. Treatment for psychological problems, psychiatric illness/behavioural disorders and social problems that might impair or endanger the security of the State and/or the Council.

29. An in-depth investigation by NIA will determine whether the reported aspects/incidents will have any influence on the security competence of the member and/or employee.

## VALIDITY PERIOD OF SECUIRITY CLEARANCES

30. Managers at all levels must ensure that a person, in respect of whom a security clearance has been issued is re-vetted (subject to the condition that such a person still occupies a post regarding the same or higher level of security clearance as the expired clearance.

31. Once issued a security clearance can be subjected to review/revision by National Intelligence Agency at any time and if necessary, be withdrawn or altered as the case may be. The rules of natural justice shall however be applied in such a case.

32. Maternity Leave. Any level of security clearance issued to female members and/or employees who go on maternity leave, remains valid on condition that the period of leave does not exceed twelve months. Should a woman resign before the confinement, she retains her clearance on condition that the interruption of service does not exceed 90 days.

33. Validity of Security Clearances Issued by Other Government Departments

a. Security clearances issued by the National Intelligence Agency (NIA), the South African Secret Service (SASS) and the South African Police Service (SAPS) shall be considered valid for the purpose of meetings and other co-operative functions.

b. A security clearance issued in respect of a member and/or employee while he/she is attached to a particular government institution is not automatically transferable to the Council or other government institution, e.g. when the member and/or employee is transferred. When a person changes his/her employer the new employer has the responsibility to decide whether an applicant's existing clearance will be accepted or whether the re-vetting of such an applicant will be required in the prescribed manner. In the case of a person from another institution

applying for a post in Matjhabeng, that person's security vetting file will be re-evaluated and a decision will be made on whether that person has to submit to re-vetting or not.

## APPLICATION PROCEDURES

34. All persons applying for the issuing re-issuing or upgrading of a security clearance shall submit their applications (completed Z204) to the Department of Public Safety and Transport.

35. Confidential Clearances

a. Applications for Confidential Clearances consist of the following documents, to be forwarded to NIA

i. Z204 and fingerprints.

ii. Consent to SAPS Criminal Record inquiry.

iii. A certified copy of the member's and/or employee's RSA identity document or passport.

iv. A covering letter from the member's and/or employee's employer, stating the post occupied/to be occupied by the member and/or employee concerned.

36. Other Grades of Security Clearance. Persons applying for all other levels of security clearance must complete the Z204, including all appendices.

37. Applications for Confidential, Secret and Top Secret clearances are to be accompanied by a covering letter from the member's and/or employee's unit/employer. Further documents to be forwarded with the application by the member's and/or employee's employer include:

a. an extract of the member's and/or employee/s conduct sheet; and

b. a report on aspects that may influence the security competence of the member and/or employee, to be completed and signed by the member's and/or employee's manager.

38. Fingerprints

a. Each application for a security clearance must be accompanied by a new set of fingerprints as vetting files are converted into microfiches.

b. Fingerprints are to be taken only by the SAPS or other authorised persons.

c. It is compulsory to complete "Indemnity by Applicant".

d. In order to prevent the compromise of information, the application must preferably be sealed by the security personnel officer before despatch.

Applications with negative recommendations and/or negative information must be sealed by the manager in person, before being despatched.

e. If a new applicant wishing to be employed by the Council does not comply with the minimum security standards, such a person may not be employed.

## VETTING PROCESS

39. Polygraph and Psychometric Tests. In accordance with the revised security vetting field work process, effective from 1 October 1996, the number of Secret or Top Secret clearances previously issued to an applicant will determine the extent to which vetting fieldwork for a clearance application will be done. The following general guidelines apply:

a. All applicants for Top Secret Clearances will be subjected to psychometric and a polygraph test regardless of their specific postings undergoing a polygraph test is a condition for the issuing of a Top Secret security clearance.

b. Applicants for any other grade of clearance will be subjected to psychometric and polygraph tests as deemed necessary, depending on the nature of information obtained by other vetting actions.

c. The polygraph should be seen as an aid in the security vetting process, and cannot cancel a thorough investigation.

d. If any applicant refuses to undergo a polygraph test, to have his/her fingerprints taken or to submit information/documentation, he/she shall be informed that a more in-depth (and possibly lengthier) investigation will have to be conducted. If a security vetting field worker is unable to make a recommendation as a result of a lack of the information, the applicant will once again be given the opportunity to give his/her voluntary co-operation.

40. Continuous Vetting. A successful security clearance process does not end when an applicant is issued with a security clearance, but must continue with frequent and productive reinvestigations. There are certain situation and requirements that necessitate productive reinvestigations. There are certain situations and requirements that necessitate re-vetting. When an individual's conduct is of such a nature that it might pose a threat to National Security or the effective protection of information in the Council re-vetting must be done.

41. Cancellation and Termination of Applications

a. In case a security clearance in process is no longer required (because of transfers, resignations, retirements, deaths. etc) NIA will be informed accordingly in writing by HOD Public Safety and Transport.

Approved/Not approved

MUNICIPAL MANAGER
R.S.B. SESELE