SECURITY POLICY

Date Approved: 30 March 2021

Council Resolution Number: E6

Contents

1. INTRODUCTION

- In addition to the following policies:
  ICT, Business Continuity Plan, Communication Plan, Disaster Management Plan, Access Control Policy and the GRDM ID card policy a security policy is the essential basis on which an effective and comprehensive security program can be developed.
- A security policy is the primary way in which management's expectations for security are translated into specific and measurable goals and objectives.
- It is crucial to take a top down approach based on a well stated policy in order to develop an effective security system.

2. PURPOSE

- A security policy is a formal statement of the rules through which people are given access to an institution's premises, assets, and technology and information assets. The security policy should define what business and security objectives management desires, but not how these solutions are engineered and implemented.
- A security policy should be economically feasible, understandable, realistic, consistent, and procedurally tolerable and also provide reasonable protection relative to the stated goals and objectives of management.
- Security policy should define the overall security and risk control objectives that Garden Route District Municipality endorses.

3. SCOPE OF THIS POLICY

3.1 This policy applies to the following (individuals and entities) resources:

- Executive Mayor, the Speaker, Mayoral Committee Members and Councilors
- The Accounting Officer, and all section 57 Managers
- All employees of Garden Route District Municipality
- All contractors, consultants and service providers delivering a service to the
- Municipality, including their employees who may interact with this institution.
- Temporary employees of the Municipality
- All information assets of the Municipality
- All intellectual property of the Municipality

- All moveable and immovable property that is owned and leased by the Municipality

3.2 The policy further covers the following seven elements of the security program of the Municipality

- Security Organization
- Security Administration
- Information Security
- Physical Security
- Personnel Security
- Information and Communication Technology (ICT) Security
- Business Continuity Planning

4. LEGAL FRAMEWORK

This policy is informed by and complies with applicable National legislation, National security policies and national security standards. A list of all applicable legislation in this regard is as follows:

- Constitution Act of South Africa , 1996 (Act 108 of 1996)
- Control of Access to Public premises and Vehicles Act, 1985 (Act 53 of 1985)
- Criminal Procedure Act, 1977 (Act 51 of 1977)
- Extension of Security of Tenure Act, 1997 (Act 62 of 1997)
- Fire-arms Control Act, 2000 (Act 60 of 2000)
- Hazardous Substances Act, 1973 (Act 15 of 1973)
- Intimidation Act, 1982 (Act 72 of 1982)
- National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
- National Archives and Record Service of South Africa Act, 1996 (Act 43 f 1996) (Previous short title "National Archives of South Africa" substituted by s. 19 of Act 36 of 2001)
- National Strategic Intelligence Act, 1994 (Act 39 of 1994)
- Occupational Health and Safety Act, 1993 (Act 85 of 1993)
- Private Security Industry Regulation Act, 2001 (Act 56 of 2001)
- Promotion of Access to Information Act, 2000 (Act 2 of 2000)
- Protected Disclosures Act, 2000 (Act 26 of 2000)
- Protection of Information Act, 1982 (Act 84 of 1982)
- Public Service Act Proclamation 103 of 1994
- Public Service Regulations of 2001, which replaced the 1999 Regulations
- Security Officers Act, 1987 (Act 92 of 1987)
- Trespass Act, 1969 (Act 6 of 1969)

- MISS Policy , 1996
- Code of Conduct for Councilors
- Code of Conduct for Staff members
- Determination of Upper limits for Councillors (Act No 20 of 1998)

5. POLICY STATEMENT

5.1 General

This policy seeks to:

- Protect the Executive Mayor, Speaker, Mayoral Committee Members, Councilors, Accounting Officer, all employees and visitors to Garden Route District Municipality against identified threats according to baseline security requirements and continuous risk management.
- To secure the information and assets of Garden Route District Municipality against identified threats according to baseline security requirements and continuous risk management.
- To ensure continued delivery of services of Garden Route District Municipality through baseline security requirements, including business continuity planning and continuous risk management.

5.2 Compliance Requirements

- All individuals mentioned in paragraph 4.1 above must comply with baseline security requirements of this policy and it's associated Security Directives as contained in the Security Plan of Garden Route District Municipality.

- These requirements shall be based on integrated security Threat and Risk Assessments (TRA's) to the interest of the Municipality and employees, information and assets of Garden Route District Municipality. The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.
- Security threat and risk assessments involve:
    - Establishing the scope of the assessment and identifying the information, employees and assets to be protected.
    - Determining the threat to information, Politicians, employees and assets of the institution and assessing the probability and impact of threat occurrence.
    - Assessing the risk based on the adequacy of existing security measures and vulnerabilities.
    - Implementing any supplementary security measures that will reduce the risk to an acceptable level.

5.3 Staff accountability and acceptable use of assets

- The Accounting Officer shall ensure that information and assets of the institution are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of Garden Route District Municipality.
- All employees, councilors and all members of the public of Garden Route District Municipality shall be accountable for the proper utilization and protection of such information and assets.
- Employees and councilors that misuse or abuse assets of the institution shall be held accountable therefore and disciplinary action shall be taken against any such employee.

6. DEFINITIONS

Access Control - The process by which access to a particular area is controlled or restricted to authorized personnel only. This is synonymous with controlled access.

Classification - The process whereby all official matters exempted from undue disclosure is labelled Confidential, Secret or Top Secret by the Manager Records /Accounting Officer or Council, having due regard to the Access of Information Manual.

Contingency Planning – The prior planning of any action that has the purpose of prevent, and or combat, or counteract the effect and results of an emergency situation where lives, property or information are threatened.

Security Communication- The conscious provision and application of security measures for the protection of classified/ sensitive communication.

Delegation- Delegation is the transfer of authority, powers or functions from one person/department to another.

Document Security- The conscious provision and application of security measures in order to protect classified/sensitive documents.

Records Management Practices- All information contained in the legislative essential registers that need to be complied with.

Employees- For the purpose of this policy the term employees includes, permanent staff, temporary, contract staff as well as councillors.

Personnel security - Personnel security is that condition created by the conscious provision and application of security measures in order to ensure that the designated person who gains access to sensitive/classified

information has the necessary security clearance, issued by the Security Officer and Head of Department and conducts himself/herself in a manner not exposing him/her or the information.

Premises/ Moveable/ Immovable property - The purpose of this policy, premises shall refer to any building, structure, shall, room, office, land, enclosure or water surface which is the property of, or is occupied by, or is under the control of the Garden Route District Municipality and to which a member of the public has a right to access .

Security - Security is the condition free of risk or danger, created by the conscious provision and application of security measures.

Security audit - That part of security control undertaken to determine the general standard of information security and to make recommendation where shortcomings are identified, evaluated the effectiveness and application of security policy/standards/procedures and to make recommendations for improvement where necessary; provide expert advice with regard to security problems experienced; and encourage a high standard of security awareness.

Security clearance - It is a process whereby an official is given access to official documents in line with the inherent requirements of the job, indicating the degree of security competence of such an official(s).

An official document that indicates the degree of security competence of a person.

Visitors - Members of the public

Contractors/Service Providers - Any individual or company rendering services to the Garden Route District Municipality, whether caterers, contractors,etc

Accounting Officer - Accounting Officer means the person who is appointed by the Council as the head of the administration and accounting officer for the Municipality in accordance with section 82 of the Structures Act.

Security Directives

- A pronouncement encouraging or banning some activities.
- A directive issued by the Council of Garden Route District Municipality; usually addressed to all heads of departments.

Security & Risk Controller

- A person in charge of efforts, such as the Municipality's communication- (in conjunction with the information technology department), access control and safety cautions to protect the Municipality (building, information, assets and

employees) against crime.

Delegation consisting of VIP's

- Any person accompany delegation where the following people are present:
    - The President
    - Members of Cabinet
    - Premiers
    - Members of Provincial Cabinet
    - Foreign delegates or diplomats
    - Mayor

7. ROLES AND RESPONSIBILITIES

7.1 The Accounting Officer

- The Accounting Officer bears the overall responsibility for implementing and enforcing the security program of the institution, towards the execution of this responsibility, the HOD: Corporate Services shall:

    - Establish the post of the Security guard and appoint a trained and competent security guard in the post.
    - Establish a security committee for the institution and to ensure the participation of all senior management, members of all the core business functions of the institution in the activities of the committee
    - Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

7.2 Head of Department

- The delegated security responsibilities lies with the Head of Department of the Municipality who will be responsible for the execution of the entire security function and program of the institution (coordination, planning, implementation, controlling, etc).
- Towards execution of his/her responsibilities, the Head of Department shall, amongst others:
    - Chair the security committee of the Municipality
    - Draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of the institution in conjunction with the security committee.
    - Review the Security Policy and Security Plan at regular intervals.
    - Advise management on the security implication of management decisions
    - Implement a security awareness program
    - Conduct internal compliance audits and inspection at the Municipality at regular intervals.
    - Establish a good working relationship with the SAPS and liaise with the institution on a regular basis.
    - As mentioned above the Head of Department should have delegated signing powers as per Municipal Manager's discretion.

7.3 Line Managers

- All managers in the Municipality shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of the Municipality.
- All managers must ensure that appropriate measures are implemented and steps are taken immediately to rectify any non -compliance issues that may come to their attention.
- This includes the taking of disciplinary action against employees if warranted.

7.4 Employees, Councilors, Contractors, Consultants and other Service Providers

- Every employee, Contractor, Consultant and other Service Providers of Garden Route District Municipality shall know what their security responsibilities are, accept it as part of their normal job function, and not only cooperate but contribute to improving and maintaining security at the institution at all times.

7.5 Stakeholders

- This policy is applicable to all members of the management, employees, consultants, contractors, councilors, visitors and any other service provider of Garden Route District Municipality.
- It is further applicable to all visitors and members of the public visiting premises of or may officially interact with the institution.

8. PRINCIPLES & CHARACTERISTICS

The security principles are an important step in security policy development as they dictate the specific type and nature of security matters most applicable to the environment of Garden Route District Municipality.
The principles here are based upon the following goals:

- Creating a safe and secure working environment for the employees of the institution;
- Creating a safe and secure environment for members of the public visiting the institution ;
- Protecting the property of the institution;
- Protecting the proprietary information of the institution.

The characteristics of a good security policy are:

- It must be **implementable** through specific procedures and directives or other appropriate methods.

- It must be **enforceable** with security tools, where appropriate and with sanctions, where actual prevention is not technically feasible.
- It must clearly define the areas of **responsibility** for the different aspects of security (security personnel, staff and management) ; and
- It must be **documented, distributed** and **communicated.**

9. GRDM SECURITY TYPES

9.1 Information security

- Categorization of information and information classification system
- The Manager Records must ensure that a comprehensive information classification system is developed and implemented in the institution.
- All sensitive information produced or processed in the institution must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.
- Employees of the institution who generates sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review.
- This responsibility includes the labeling of classified documents.
- The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times.

9.2 Physical Security

- Physical security involves the physical layout and design of facilities of Garden Route District Municipality and the use of physical security measures to delay and prevent unauthorized access to assets of the institution.
- It includes measures to detect attempted or actual unauthorized access and the activation of an appropriate response.
- Physical security also includes the provision of measures to protect employees from bodily harm.
- Physical security measures must be developed, implemented and maintained in order to ensure that the entire Municipality, its personnel, property and information are secured.
- These security measures shall be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Guard.
- Garden Route District Municipality shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities.
  The Municipality shall:

- Select, design and modify facilities in order to facilitate the effective control of access thereto.
- Demarcate restricted areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto.
- Include the necessary security specifications in planning, request for proposals and tender documentation.
- Incorporate related costs in funding requirements for the implementation of the above.

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

9.3 Personnel Security Screening

- All newly appointed employees, councilors, contractors and consultants attached to Garden Route District Municipality, who requires access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security screening investigation.
- A declaration of secrecy shall be signed by every individual issued with a security clearance to complement the entire security screening process. This will remain valid even after the individual has terminated his/her services with the Municipality.
- A security clearance will be valid for a period of ten years in respect of confidential level and five years for Secret and Top Secret.
- This does not preclude re-screening on a more frequent basis as determined by the Accounting Officer, based on information which impact negatively on an individual's security competency.
- Security clearances in respect of all individuals who have terminated their services with the Accounting Officer shall be immediately withdrawn.

9.4 Information and Communication Technology (ICT) Security

ICT Security

- Approved ICT policies of Council
- All relevant systems will be secured as per ICT approved Policies of Council."

10. IMPLEMENTATION

- The Accounting Officer, HOD: Corporate Services and the appointed Security guard are accountable for the enforcement of this policy.
- All employees and councilors of the municipality are required to fully comply with this policy and its associated Security Directives as contained in the Security Policy.
- Non-compliance with any prescript shall be addressed in terms of the Disciplinary Code/Regulations of the Municipality.
- Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of the municipality shall be included in the contracts with such individual/institutions/companies.
- The consequences of any transgression/deviation or non-compliance shall be clearly stipulated in the said contract and shall be strictly enforced. Such consequences may include the payment of prescribed penalties or termination of the contract, depending on the nature of any non-compliance.

10.1 Exceptions

- Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:

    - When security must be breached in order to save or protect the lives of people.
    - During unavoidable emergency circumstances e.g. natural disasters.

10.2 Other considerations

- The following shall be taken into consideration when implementing this policy:

    - Subject to Government Regulations promulgated regarding disasters, world pandemics, emergency actions and unrest this policy can be amended
    - Occupational Health and Safety issues of Garden Route District Municipality
    - Disaster Management of the Garden Route District Municipality.
    - Disabled people shall not be inconvenienced by physical security measures and must be catered for in such a manner that they have access without compromising security or the integrity of this policy.
    - Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).

11. POLICY REVIEW

11.1 Review and update process

- The Manager must ensure that this policy and its associated Security Directives is reviewed and updated on an annual basis.
- Amendments shall be made to the policy and directives as the need arise.

12. PROCESSES

12.1 Security administration

The functions referred to in above include:

- General security administration (departmental directives and procedures, training, and security awareness, security risk management, security audits, sharing of information and assets)
- Setting of access limitations
- Administration of security screening
- Implementation of physical security
- Ensuring the protection of employees
- Ensuring the protection of information
- Ensuring ICT security
- Ensuring security in emergency and increased threat situations
- Facilitating business continuity planning
- Ensuring security in contracting
- Facilitating security breach reporting and investigations
- Implementation Strategy.

12.2 Security incident/breaches reporting process

- Whenever employees and councilors of the institution become aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidental or intentional), they must report this to the Security guard of the institution by utilizing the formal reporting procedure prescribed by the Security Breach Directive of the institution.
- The Security guard shall report to the appropriate authority (as indicated in the Security Breach Directive) of the institution all cases or suspected cases of security breaches for investigation.

- The Security guard of the institution shall ensure that all employees and councilors are informed about the procedure for reporting security breaches.

13. REFERENCES

- Approved ICT policies of Council
- All relevant systems as secured as per ICT approved Policies of Council
- Draft Access Control Policy