Garden Route

DISTRICT MUNICIPALITY | UMASIPALA WESITHILI | DISTRIKSMUNISIPALITEIT

GRDM ACCESS CONTROL POLICY

Date Approved:	**29/03/2022**	Council Resolution (DC No):	**E.3**

Contents

1. Introduction

- The Garden Route District Municipality (GRDM) Access Control policy is to provide guidelines and standards for the management of access to all GRDM buildings/offices, premises, resorts and other properties belonging to the municipality.

- Physical security includes the protection of people, property, and physical assets from actions and events that could cause damage or loss.

- The responsibility of physical security is firstly to ensure the safety of Councillors, employees, visitors and the public when they access GRDM properties.

- Legislation prescribes that the municipality must establish controls and systems to regulate the appropriate and efficient use of municipal resources.

- This Policy ensures that all assets of GRDM are protected at all times.

- The GRDM Access Control Policy forms part of the GRDM Security Policy.

2. Legal Framework

- Control of Access to Public Premises and Vehicles Act, Act No 53 of 1985.

- Code of Conduct for Municipal officials

- Code of Conduct for Councillors

3. Purpose of this Policy

The purpose of the policy is to control physical access at GRDM buildings and premises including the resorts and other GRDM properties. This also indicates access to certain restricted areas located within buildings.

The purpose of an access control system is to provide quick, convenient access to authorized persons, while at the same time restricting access to unauthorized people.

Furthermore, the purpose of the Physical Access Control Policy is to:

- Establish the rules for granting, control, monitoring, and removal of physical access to office premises; to identify sensitive areas within the municipality and to define and restrict access.

4. Scope of this Policy

The policy applies to:

- All permanent employees of the municipality
- All contract employees
- Councillors
- Students/Interns
- Public
- Service Providers; and
- National and Provincial Government employees/visitors

5. Key Principles

- Physical control measures at GRDM buildings/premises include all types of building materials, fencing, locks, and guards.

- Deterrence, denial, detection then delay are the controls used for securing the environment.

- Components of security are access control, surveillance, and security testing, which work together to ensure safety at GRDM.

6. Components of Access Control

At a high level, access control is about restricting access to a resource. Access controls have five main components:

- **Authentication:** The act of proving an assertion, such as the identity of a person.

- **Authorization:** The function of specifying access rights or privileges to resources.

- **Access:** Once authentication and authorization is completed, the person can access the building.

- **Manage:** Managing an access control system includes adding and removing authentication and authorization of users or system.

- **Audit:** Regular and continuous audit of current procedures and processes.

7. Risk analysis

It is essential that all municipal services is conducted in an environment where potential threats (including those from both natural and human-made hazards, terrorism, crime and insider threats) to GRDM assets, information and personnel etc. have been identified, risk assessed and appropriately mitigated to prevent interference, loss or compromise (malicious or otherwise).

This includes ensuring physical perimeters and entry controls are in place to provide proportionate protection against natural disasters, forced entry and terrorist attacks.

8. Roles and Responsibilities

Secure areas are protected by appropriate entry and controls for authorized personnel.

- Procedures exist that establish visitor controls including visitor sign-in logs and wearing of visitor badges for both entry and exit of the GRDM buildings/offices.

- Policies specify management's review of the list of individuals with physical access to facilities containing sensitive information (whether in paper or electronic forms).

- A complete inventory of critical assets is maintained with GRDM ownership defined and documented.

- Card access records and visitor logs for buildings are kept for periodic review based upon the criticality of the information being protected and security necessity.

- All employees, contractors, service providers, councillors and employees of other organisation who are on GRDM premises and co-located sites remain accountable for the security, health and safety of themselves, colleagues, and the protection of municipal assets.

- The Access Controllers together with their supervisor and relevant HOD has the responsibility for ensuring physical access and annual risk assessments.

- The Access Controllers/Supervisor and HOD Corporate Services must ensure the action plans created to address identified risks and instigate business continuity activities are up-to-date, clearly communicated, regularly rehearsed, implemented effectively and readily available in accordance with their significance/importance/classification.

- Managing the physical access controls of sites (e.g. perimeter control, guarding, site access etc.) occupied by GRDM employees is the responsibility of the Access Controllers in cooperation with Supervisor and HOD Corporate Services.

- Measure the controls in the form of annual access control reviews undertaken by Access Controllers, Supervisor and HOD of Department.

- It will be the responsibility of the designated officials to procure the correct equipment for such physical access control measures to ensure that the most recent technical/industry standards are met and that the technology and processes in place are regularly reviewed to ensure that the access controls remain effective and fit for purpose.

- The designated officials must also ensure that the technical/industry standard for the Surveillance Cameras are met to monitor access control is in place.

9. Access Control points

9.1 Head Office, 54 York Street George

- Access to Head Office parking area at back entrance is only by GRDM ID Card.

- GRDM officials to enter the building via back entrance only by GRDM ID Cards only.

- GRDM officials to enter the building via front entrance only by GRDM ID Cards.

- Access of Public/Visitors/Service Providers done by the Access Controllers on duty.

- Visitors/service Providers/Public to sign attendance register at entrance before proceeding into the building.

- GRDM official to accompany them to office/committee room or other.

- GRDM employees/Visitors/Public and Service Providers to enter through metal detectors placed at front entrance.

- Declaration of possession of weapons or other sharp objects to Access Controllers before access is granted.

- ICT entrance restricted to ICT officials only.

- Access control of buildings and offices after hours should be via the GRDM ID Cards.

9.2 Community Services at Mission Street George

- Access to premises is controlled by private security guards at entrance.
- Visitors/Public/ Service Providers and Government officials to sign attendance register at gate.
- Entrances to Community Services building are controlled.

9.3 Roads Department at Mission Street George

- Access to Roads Department premises is controlled by private security guards at the entrance.
- Visitors/Public/Service Providers and Government officials to sign attendance register at gate.
- Entrances to Roads Department buildings are controlled.

9.4 Stores at Mission Street George

- Access to premises of Stores section is controlled by private security guards at the entrance.
- Access control to building at Stores section is only by GRDM ID Card.
- Entrance to Store section is controlled by GRDM officials that receive incoming stock.

9.5 Fire Services George

- Access control at two entrances to the building by Fire Services employees.

10. Access Control Processes

10.1 Key Access and Card Systems

The following policy applies to all facility access cards/keys:

Employee access cards and/or keys must not be shared or loaned to others.

Access cards/keys shall not have identified information other than a return mail address and all cards/keys that are no longer required must be returned to ICT.

Lost or stolen cards/or keys must be reported immediately to ICT.

ICT shall remove card and/or key access rights of individuals that change roles or are separated from their relationship with GRDM; and

The Supervisor or the designee regularly reviews access records and visitor logs for the facility and is responsible for investigating any unusual events or incidents related to physical facility access.

10.2 VISITOR AND GUEST ACCESS

The following procedures apply to identification and authorization of visitors and guests to the GRDM:

- Any facility that allows access to visitors shall track visitor access with a sign in/out log.
- A visitor log shall be used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centres' where sensitive information is stored or transmitted.
- The visitor log shall document the visitor's name, the firm represented, and the on-site personnel authorizing physical access on the log.
- The visitor log shall be retained for a minimum of three months, unless otherwise restricted by rule, regulation, statute, or audit control.
- Visitors shall be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from on-site personnel.
- Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration.
- Visitors shall be authorized before entering, and escorted at all times within, areas where sensitive information is processed or maintained.
- Visitors must be escorted in card access-controlled areas of facilities.

10.3 Confidential Area Access

The following procedures pertain to access to confidential areas:

- All areas containing sensitive information shall be physically restricted
- All individuals in these areas must wear an identification badge on the person so that both the picture and information on the badge are clearly visible to personnel
- Restricted IT areas such as data centres, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing IT resources shall be restricted based upon functional business need
- Physical access to records containing sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted

- Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information
- Appropriate facility entry controls shall limit and monitor physical access to information systems
- Surveillance cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas and this data shall be stored for at least three months, unless otherwise restricted by rule, regulation, statute, or law
- ICT staff shall:
- Implement physical and/or logical controls to restrict access to publicly accessible data jacks (for example, data jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized)
- Ensure visitors are always escorted in areas with sensitive information
- Areas accessible to visitors should not have enabled data jacks unless network access is provided to a secure guest network only
- Restrict physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines
- Control physical and logical access to diagnostic and configuration ports
- Receive prior authorization before disposing, relocating, or transferring hardware, software, or data to any offsite premises

10.4 Physical Site Access

On-site physical access to sensitive or confidential areas for shall be controlled though a combination of the following mechanisms:

- Security based on individual job function
- Revocation of all facility access immediately upon termination and collection of keys, access/smart cards, and/or any other asset used to enter facilities
- Policies and procedures shall be established to ensure the secure use, asset management, and secure repurposing and disposal of equipment maintained and used outside the organization’s premises.

10.5 Contractor Requirements

External contractors shall comply with applicable laws and regulations regarding security and background checks when working in facilities. For unclassified personnel, an appropriately cleared and technically knowledgeable staff member shall escort the individual to the area where facility maintenance is being performed and ensure that appropriate access control and procedures are followed:

- Any system access, initiation or termination shall be performed by the escort
- Keystroke monitoring shall be performed during access to the system
- Prior to maintenance, the information system is completely cleared, and all non-volatile data storage media shall be removed or physically disconnected and secured
- Maintenance personnel must not have visual or electronic access to any sensitive or confidential information contained on the system they are servicing
- Devices that display or output sensitive information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information
- All personnel granted unescorted access to the physical area containing the information system shall have an appropriate security clearance

10.6 Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of normal operations. Examples of acceptable controls and procedures include:

- Visitor logs
- Access control procedures and processes
- Operational key-card access and premise control systems
- Operational video surveillance systems and demonstrated archival retrieval of data

10.7 Enforcement

Staff members found in policy violation may be subject to disciplinary actions.

11 References

- Approved ICT policies of Council
- All relevant systems as secured as per ICT approved policies of Council
- Security Policy

12 Policy Review

The GRDM Policy review will take place annually and submitted to Council for approval.