



FINAL

ACCESS CONTROL POLICY

2026-2027

CONTENTS

Physical Access Control Policy.....	3
Purpose.....	3
Strategy.....	3
Roles and responsibilities	3
Policy.....	4
Enforcement	5
Logical Access Control Policy.....	5
Purpose.....	5
Scope.....	5
Responsibilities.....	5
Policy.....	6
Enforcement	7
Annex A – Request For Access Form.....	8
Annex B – Service provider Request for Access Form	

PHYSICAL ACCESS CONTROL POLICY

PURPOSE

The purpose of the Physical Access Control Policy is to govern access to buildings owned and/or rented by the Municipality and as such to protect the Municipality against unauthorised access to, theft of, or deliberate damage to its IT assets.

STRATEGY

The Municipality aims to protect against the threads of unauthorised access to its IT assets by means of:

- Defining a list of mission critical IT server rooms inside the organisation
- Clearly defining personnel authorized to enter IT server rooms
- Logging all entries and exits into all IT server rooms
- Collecting and providing evidence of the movement of staff into and out of Municipality owned buildings and buildings rented by the Municipality for operations

ROLES AND RESPONSIBILITIES

CHIEF FINANCIAL OFFICER

- Shall ensure the installation and operation of electronic physical access control systems at the entry and exit points of all defined IT Server Rooms.
- Shall ensure that all authorized personnel are either:
 - provided with a uniquely identifiable pin that can be used to access the defined server rooms, and/or
 - an identification device that can be used to access the defined server rooms, and/or
 - can be identified by means of acceptably secure electronic recognition systems installed at the entry/exit points of the Server Rooms (i.e., fingerprint recognition and retina recognition)
- Shall be responsible for authorization by means of approval or rejection of service providers and internal employees that request temporary access to the server rooms
- Shall process applications for employee registrations on the access control systems
- Shall provide reporting of physical access to the server rooms
- Shall process termination of access control requests
- Shall be responsible for authorization of any repairs to the access control system in the event of an access control system failure

THE IT SERVICE PROVIDER

- Shall ensure that the physical access control systems are fully operational
- Shall oversee any maintenance and/or repair work that needs to be done to ensure the operation of the physical access control systems
- Shall facilitate and log temporary requests for access to the server rooms by individuals duly authorised by the Municipality to gain temporary access to the server rooms

THE DIRECTORS OF EACH DIRECTORATE

- Shall request access permissions on behalf of each member of their staff by completing the “Request for Access” form attached in Annexure A to this policy
- Shall within 24 hours of termination of service of a staff member in their directorate, request termination of access control by logging an official request in the IT helpdesk

ALL PERSONS WITH ACCESS PERMISSIONS

- Shall be responsible for the handling and safekeeping of their access control device, if supplied with such a device
- Shall be responsible for the confidentiality of their PIN codes, if supplied with a pin code
- Shall report within 24 hours to their line function manager or CFO the loss of their access control device, or the suspicion of leakage of their PIN code.
- Shall immediately upon separation with the municipality, return their access control device to the Municipality

POLICY

- All employees and councillors with designated office space in any particular Municipality owned or rented building shall be provided with a means of identifying themselves with the access control system if installed.
- Employees and councillors will, by default, only have access to the areas inside the buildings which is required for them to perform their official duties.
- Employees and councillors can only gain access to additional areas if officially approved to do so.
- Service providers upon request will be provided temporary access to perform their authorised duties.
- Lost and physically damaged access control devices will be replaced at the device holder’s expense.
- Malfunctioning access control devices will be replaced at the expense of the municipality.
- No person may be issued with more than one functioning access control device at any given time.
- No person may at any time lend his/her access control device to any other person.
- No person may at any time provide his/her pin code (if applicable) to any other person.

- Any person that chooses to ignore this rule will be held responsible for all actions of the person(s) in possession of his/her pin code. No person may use any means whatsoever to attempt to bypass the access control system other than for the purpose of authorized repairs to the access control system if it fails.
- Records produced by the access control system shall be regarded as official records and as evidence of the movements of the identified person.

ENFORCEMENT

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- Any service provider or contractor found to have violated this policy may be subject to termination of its service contract.
- Any person that lends his or her Municipality-issued access control device to another person may be held responsible for any and all actions of such person(s), and persons to whom they hand the device, while they are in possession of his/her access control device.
- Any person that provides another person with his/her pin code may be held responsible for all actions of the person(s) in possession of his/her pin code, and any persons to whom they give the pin code.

LOGICAL ACCESS CONTROL POLICY

PURPOSE

To govern the unique identification of users granted with access to systems inside the Municipal IT infrastructure, thereby enhancing the confidentiality and integrity of information stored in the systems deployed by the Municipality.

SCOPE

This policy applies to all entities including but not limited to officials, politicians, contractors and service providers, permanent and temporary workers that may require access to any system deployed by any department on any part of the Municipality's IT infrastructure.

RESPONSIBILITIES

MUNICIPAL MANAGER/DIRECTORS/MANAGERS

- Each director/manager is responsible for requesting access of all users inside their department or unit to relevant systems hosted by the Municipality. This is done by completing, signing and submitting a "Request for Access" form (RFA001 annexed hereto) and submitting it to their senior Manager for approval and onward submission to the CFO for processing.

- Each Senior Manager/The Municipal Manager is responsible for approving the access of all users in the Municipality to systems hosted on the Municipal IT infrastructure, for which the Municipal Manager, Senior manager or Section Head is responsible.

HUMAN RESOURCES

- The Human Resources Department shall, within 24 hours of termination of service of an employee, regardless of whether permanent or temporarily, be responsible for sending an email to the IT Helpdesk requesting termination of access rights of such employees.

CHIEF FINANCIAL OFFICER

- Shall process all "Request for Access" forms (RFA001 annexed hereto).
- Shall process all "Temporary User Access Request" forms (RFA002 annexed hereto).
- Shall forward relevantly portions of the "User Access Request" forms to the managers of the individual systems for approval.
- Shall, upon approval from the system managers, log an official request in the IT helpdesk for the user access to be granted.
- Shall process all requests for termination of access rights:
 - Log an official request in the IT helpdesk for the user domain access rights to be terminated
 - Request that the system managers terminate each individual right that the user held, and
 - Upon completion report back to the Human Resources Department.

THE DOMAIN ADMINISTRATORS

- Shall, upon receipt of an approved "User Access Request" form:
 - Create the new user account on the domain (if this is a new user) and assign the requested access rights to the account.
 - Review the existing domain access rights (if this is an existing user).
 - Report back to the requesting Senior Manager upon completion, with evidence of the creation of the new domain user account and the assigned rights.
- Shall, upon receipt of a request for termination of user access rights:
 - Disable the user account in the domain for a period of 30 days.
 - Delete the user account from the domain after 30 days have expired.
 - Report back to the Chief Finance Officer who will notify the Senior Manager: Corporate Services on completion of both events to inform the Human Resource Department.
- Shall conduct monthly checks to verify synchrony between users and access roles.
- Shall, in writing report any deviations from the policy that were found.

POLICY

Access to systems will only be granted where there is a clearly established business need, which is consistent with the roles and responsibilities of those granted access.

Access rights will be assigned based on the roles of the user or system that requires access. Each job function requires that users or applications have a specific level of access to each system (i.e., Operating Systems, databases, applications).

Each job function will have its own distinct access role, and all users or applications having the same job function will have the same access roles.

Users and applications are granted "least privilege" access to resources.

If a group of users with the same job function require additional access due to the expansion of their job function, the existing access role will be modified to reflect the job function expansion.

If an individual in a group acquires an additional job function that is different from the group job function, then that user must be assigned an additional access role.

If an appropriate access role does not already exist, a new access role will be created to accommodate that individual.

No functional users will be assigned administrator level access to any of the Production servers.

Only IT Administrators will have access to software configuration data.

Development personnel and other external providers, other than any service provider deemed as outsourced IT Administrators will not have updated access to Production servers.

Users shall not attempt to bypass logical security mechanisms including but not limited to bypassing access controls by logging in using another user's account or by logging in using a group or application account.

All user-IDs will comply to the following rules:

- User ID's must be at least five characters long unless a user's actual name and/or surname contains less than 5 characters, in which case it may be changed to the user's actual name/surname of less than 5 characters.
- User ID's must be descriptive of a person, not a job function

No one shall grant, enable, disable, modify or revoke a user's access unless the request was submitted in writing by an authorized requestor.

ENFORCEMENT

- Any person gaining any access to the systems deployed on the Municipal infrastructure will be required to act in compliance with this policy.
- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- Any service provider or contractor found to have violated this policy may be subject to termination of its service contract.

ANNEX A – REQUEST FOR ACCESS FORM

Emthanjeni Municipality

RFA-001

Request for Access Form

General

Date

Request Type New Change to employee with username



For changes to existing employees, please complete only the information that needs to be changed and cross out all fields that are not filled in.
For new employees, please complete all sections.

Personal Information

Title Mr Mrs Miss Ms

Name

ID Number Employee No

Telephone Fax

Position

Job Title

Department

Reporting To

Location De Aar Hanover Britstown Other Specify:

Type Full time Temporary From To

Additional Information

Senior Manager Signature

Emthanjeni Municipality

RFA-001

Request for Access Form

Statutory Required Information

Gender	<input type="checkbox"/>	Male	<input type="checkbox"/>	Female	
Race	<input type="checkbox"/>	Caucasian	<input type="checkbox"/>	Indian	<input type="checkbox"/> Coloured
	<input type="checkbox"/>	Asian	<input type="checkbox"/>	African	
	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No	
Occupational Category	<input type="checkbox"/>	Top Management			
	<input type="checkbox"/>	Senior Management			
	<input type="checkbox"/>	Professionally qualified, experienced specialists and mid-management			
	<input type="checkbox"/>	Skilled technical and academically qualified workers, junior management, supervisors, foremen, superintendents			
	<input type="checkbox"/>	Semi-skilled and discretionary decision making			
	<input type="checkbox"/>	Unskilled and defined decision making			

Senior Manager Signature

Emthanjeni Municipality

RFA-001

Request for Access Form

Physical Access to Buildings and Facilities

Buildings	<input type="checkbox"/>	Main Building	<input type="checkbox"/>	Engineering	<input type="checkbox"/>	Electro Technical
	<input type="checkbox"/>	Finance	<input type="checkbox"/>	Traffic	<input type="checkbox"/>	Council Chambers
	<input type="checkbox"/>	Cashiers	<input type="checkbox"/>	Stores	<input type="checkbox"/>	Traffic
	<input type="checkbox"/>	Library	<input type="checkbox"/>		<input type="checkbox"/>	Workshop
Server Rooms	<input type="checkbox"/>	Finance	<input type="checkbox"/>		<input type="checkbox"/>	



Please apply the principle of "least access". No access to server rooms will be approved without a written justification.

Senior Manager Signature

Office Use

Approved By

Completed By

Date

Date

Signature

Signature

Emthanjeni Municipality

RFA-001

Request for Access Form

Domain Account

Require a network user account?

Yes No

Building in which the employee will work

Office Number

Computer Available?

Yes No

Printer Available?

Yes No

Printer Required?

Yes No

Network Point Available?

Yes No

The employee requires access to:

Zimbra (E-mail)

Yes No

CCG System

Yes No

PAYDAY

Yes No

Performance Management

Yes No

Senior Manager Signature

Office Use

Account Name

Approved By

Completed By

Date

Date

Signature

Signature

Emthanjeni Municipality

RFA-001

Request for Access Form

PHONIX FMS Access

Billing	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No
Ledger	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No
Assets	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No
SCM	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No
Cashbook	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No

PHONIX FMS - Super User

Require Administrative Privileges? Yes No

Justification

Senior Manager Signature

Office Use

Account Name	<input type="text"/>		
Approved By	<input type="text"/>	Completed By	<input type="text"/>
Date	<input type="text"/>	Date	<input type="text"/>
Signature	<input type="text"/>	Signature	<input type="text"/>

Emthanjeni Municipality

RFA-001

Request for Access Form

Ignite Account

Active User	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No			
Complaints Assist	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No			
Performance Assist	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No			
Section 57	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No			
Staff	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No			
HR	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No			
Job Level	<input type="text" value="T"/>			Job Number	<input type="text"/>		
Development	<input type="checkbox"/>	Activation	<input type="checkbox"/>	Evaluation	<input type="checkbox"/>	Reporting	
Agreement	<input type="checkbox"/>	Activation	<input type="checkbox"/>	Evaluation	<input type="checkbox"/>	Reporting	
Section 57 Appointees	<input type="checkbox"/>	Activation	<input type="checkbox"/>	Evaluation	<input type="checkbox"/>	Reporting	
Resolution Assist	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No			
Task Assist	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No	Update: <input type="checkbox"/>	Own Actions <input type="checkbox"/>	All Actions
SDBIP	<input type="checkbox"/>	Yes	<input type="checkbox"/>	No	<input type="text" value="List of Previous Book Years to which access is required"/>		

Senior Manager Signature

Office Use

Account Name	<input type="text"/>		
Approved By	<input type="text"/>	Completed By	<input type="text"/>
Date	<input type="text"/>	Date	<input type="text"/>
Signature	<input type="text"/>	Signature	<input type="text"/>

Emthanjeni Municipality

RFA-001

Request for Access Form

Zimbra Account Information

Request type

New

Change to email account

e-mail address

Type of change

Description

Add additional Aliases
to this account?

Yes

No

e-mail alias here

e-mail alias here

Mailbox Quota (Select
One)

Use Standard Mailbox Quota

Increase Mailbox Quota to:

Justification for larger quota

Senior Manager Signature

Office Use

Approved By

Completed By

Date

Date

Signature

Signature

Emthanjeni Municipality

RFA-001

Request for Access Form

Internet Access Information

Unlimited Internet Access

Limited Internet Access

Specify website(s) below:-

Senior Manager Signature

Office Use

Approved By

Completed By

Date

Date

Signature

Signature

Emthanjeni Municipality

RFA-001

Request for Access Form

Management Authorization



To be completed and signed by the employee's Manager.

I hereby declare that:

- The information completed in this application form is correct.
- I am duly authorized to submit this application for this employee.
- I have signed each page of this application form.
- The employee for whom this application form was completed was presented with and has accepted all IT policies of the Emthanjeni Municipality.
- I authorize that the access permissions for this employee may be created as requested in this form.
- I understand that the request is subject to approval from the responsible managers in charge of each system and/or resource for which access permissions is requested.

Snr. Manager/Section Head Name

Capacity

Date

Signature

Emthanjeni Municipality

RFA-002

Service Provider Request for Systems Access Form

Applicant Detail

Title	<input type="checkbox"/> Mr	<input type="checkbox"/> Mrs	<input type="checkbox"/> Miss	<input type="checkbox"/> Ms		
Name	<input type="text" value="Full Names"/>			<input type="text" value="Surname"/>		
ID Number	<input type="text"/>		Telephone	<input type="text"/>		
Capacity	<input type="text"/>		Employer	<input type="text"/>		

Request for Systems Access

Type Of Access	<input type="checkbox"/> VPN	<input type="checkbox"/> Physical Access
From	<input type="text" value="YYYY/MM/DD - HH:MM"/>	
To	<input type="text" value="YYYY/MM/DD - HH:MM"/>	

Which systems do you need access?

CCG ERP	<input type="checkbox"/> Yes	<input type="checkbox"/> No
PAYDAY	<input type="checkbox"/> Yes	<input type="checkbox"/> No
System	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Other (explain below)	<input type="checkbox"/> Yes	<input type="checkbox"/> No

