



GREATER GIYANI MUNICIPALITY

Tel : 015 811 5500
Fax : 015 812 2068
Web : <http://www.greatergiyani.gov.za>

P/Bag X 9559
Giyani
0826

I T NETWORK ACCESS POLICY

1st approval : Council Resolution no# CR17-31/10/13SC (4)
2nd approval : Council Resolution no# CR89-29/05/19SP
3rd approval : Council Resolution no# CR97 – 28/05/21 SP
4th approval : Council Resolution no# CR133 – 27/05/22 SP

Object

The purpose of this policy is: -

- (a) To put controls in place by controlling who has the right to use what type of information and.
- (b) Guarding against unauthorized use and access to information

TABLE OF CONTENTS

PAGES

1. GLOSSARY..... 03

2. PREAMBLE..... 04

3. USER AWARENESS..... 04

4. PURPOSE..... 04

5. DOCUMENTS THAT SHOULD BE READ WITH THE POLICY..... 04

6. SCOPE OF APPLICABILITY OF THE POLICY..... 05

7. ROLES AND RESPONSIBILITIES..... 05

8. ENFORCEMENT/LEGAL FRAMEWORK..... 05

9. POLICY..... 06

9.1 Network Access 06

9.2 User Account and Password Management 07

9.3 Remote Access Connection 08

9.4 Server Access 08

9.5 Client Data Access 08

10. POLICY REVIEW..... 09

1. GLOSSARY

“**GGITO**” Refers to Greater Giyani Information Technology Office staff members.

“**IT**” refers to Information Technology.

“**GGITO- IT security Policy**” refers to greater Giyani Information Technology Office Information Technology Security Policy.

“**GGM**” refers to Greater Giyani Municipality.

“**MBSA**”

“**Network Devices**” refers to computers and devices interconnected by communications among users.

“**The municipality**” refers to Greater Giyani Municipality.

“**IR**” refers to Information Resources.

“**HR**” refers to Human Resource Management Division.

“**MFC**” refers to Multi-Function Copier

“**email**” refers to electronic mail

“**UPS**” refers to Uninterrupted Power Supply

“**BCP**” refers to Business Continuity Plan

“**DRP**” refers to Disaster Recovery Plan

“**MM**” refers to Municipal Manager

“**SLA**” refers to Service Level Agreement

“**Workstation**” refers to computers and laptops.

2. PREAMBLE

- (a) The Greater Giyani Information Technology office (GGITO) has developed the Network Access Policy to establish specific requirements for accessing GGM IR.
- (b) This policy shall apply to all Greater Giyani Municipality's officials, its contractors, service providers, interns, students, councillors, and other authorised 3rd party entities that will need the municipality's IT Network in order to perform respective duties on the network of GGM.
- (c) The purpose of this policy is to protect the municipality's Information Technology Resources and to safeguard the confidentiality and integrity of information, resources, data, ICT equipment and council documentations.
- (d) GGITO Network Access Policy protects GGM IR from accidental and/or negligent detection, destruction and modification GGITO will put in place controls that will control who will have access to what type of information and determine privilege levels of each information user.
- (e) Formal procedures should be put in place to control how GGM IR is accessed and control how changes to information are affected.
- (f) Modification and/or destruction of information should have an audit trail.

3. USER AWARENESS

- (a) Every councillor, employee, contractor and authorised 3rd party entity should become familiar with this policy's provisions and the importance of adhering to it when using the Municipality's computers, network, data and other information resources.
- (b) Each is responsible for reporting any suspected breaches of its terms to the IT Manager security.
- (c) Popularization of this policy will be conducted through presentations to all staff members.
- (d) All officials shall attend presentations of this policy and sign on attendance register as acknowledgement of knowledge of this policy and repercussions of transgression.

4. PURPOSE

The purpose of this policy is to put controls in place by controlling who has the right to use what type of information and guarding against unauthorized use and access to information.

5. DOCUMENTS THAT SHOULD BE READ WITH THE POLICY

- (a) Formal procedures must be put in place to control how access is granted and how such access is changed and the period of such access.
- (b) The policy also mandates a standard for creation of strong passwords, passwords protection and frequency of changing passwords.
- (c) Password Policy

- (d) Change Management Policy
- (e) ICT Equipment Policy
- (f) Network Access Policy
- (g) IT Security Policy
- (h) COBIT 5- Framework for the Governance and Management of Enterprise IT 2012
- (i) ISO/IEC 20000
- (j) ISO/IEC 27000
- (k) KING IV – Corporate Governance of Information and Communication Technology (ICT)
- (l) ITIL v3

6. SCOPE OF APPLICABILITY OF THE POLICY

This policy applies to every network user of GGM including and not limited to councillors, staff members, third party service providers, partners, interns, contract workers, service, and agents

7. ROLES AND RESPONSIBILITIES

- (a) GGITO is responsible for monitoring for ensuring that IR is maintained in compliance with the Municipality's Network Access policy and procedures.
- (b) The IT Manager is responsible for monitoring compliance to the Municipality's Network Access policy.
- (c) All GGITO Team members are responsible to make sure that they adhere to GGITO Network Policy and the enforcement the policy.
- (d) HRM's will alert GGITO of new Network Access needs whenever new appointment are made and inform GGITO when employees cease under the employ of GGM.
- (e) IT is the user's responsibility to ensure that they safeguard their passwords in order to prevent their password being used to gain unauthorised access to the network.
- (f) It is the user's responsibility to ensure that they do not leave their computers active while not attended they must either lock it or logoff.

8. ENFORCEMENT/LEGAL FRAMEWORK

- (a) Any employee found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.
- (b) Employees who violate this policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations, and policy prescripts (this list is by no means exhaustive):
 - (i) The state Information Technology Act

- (ii) SITA Amendment Act
- (iii) Promotion of Access to information Act
- (iv) Municipal Service Act
- (v) Municipal Finance Management Act
- (vi) National Archives Act
- (vii) Protection of Government Information Act
- (viii) Telecommunication Act
- (ix) Electronic Communication and Transaction Act
- (x) Various other statutes
- (xi) Any other application legislation, regulation or policy

9. POLICY

(1) Network Access

- (a) Formal user access control be documented, implemented and kept up to date for application and information system to ensure authorized user access and prevent unauthorized user access.
- (b) The process and physical access must be documented from the moment the user is registered on the network until the time the user is deregistered on the network.
- (c) Each user must be granted access and rights according to their needs and job.
- (d) Each user access rights must be reviewed regularly to ensure that appropriate rights are granted to the right persons.
- (e) Only GGITO officials must have administrative rights and they must be recorded as such. Any other person that needs to have administrative rights will be recorded and the rights will be removed at the end of the session
- (f) All third-party vendor physical access to server and switch room must be logged in a register in the format (Name, Surname, Company, Purpose, Data and Time) and must be accompanied by a GGITO official at all times.
- (g) Third party service providers will only be granted controlled access to remotely access the network by Manager IT under strict supervision by GGITO.

9.1 User Account and Password Management

- (1) Each employee that requires access to GGM network shall be accompanied by HRM official to GGITO offices for registration of user account.
- (2) Each application form will be accompanied by the employee's appointment letter for approval by IT Manager.
- (3) No network access shall be granted to unauthenticated individuals.
- (4) When the employee cease to work for GGM it is the responsibility of HRM line Manager to inform GGITO of such termination of employment and GGITO will suspend the account of such user.

- (5) GGITO shall not terminate any user account without being informed by the HRM line Manager of such need to terminate. HRM shall on regular bases send approved termination register to GGITO to effect such terminations on Active Directory Exchange.
- (6) All accounts shall be reviewed at least quarterly to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status
- (7) The HRM will ensure that GGITO be informed at least one month in advance of any new appointments. No user account will be created or modified without a signed new/Modified User Form
- (8) All user accounts will be deleted, and mailboxes deleted immediately by the GGITO, upon an employee's departure from the Municipality either by dismissal, transfer, resignation, retirement, death or any other forms of departure as informed by HRM line Manager. There shall be system to record terminations and new appointments and such information will form part of GGITO monthly reports.
- (9) An employee's access to user account will be changed/modified by GGITO, once the employee has transferred to a different division; in accordance with the employee's new job functions and requirements as advised by HRM line Manager
- (10) All user accounts at the Municipality are created as standard User accounts. This means that the users have standard privileges to log on to the network, use network printers that have been assigned to them, access their email, and use the internet and any other privilege that is a core requirement of the job function.
- (11) Usernames are standardized and the employee's unique employee number is used to enable user to log on to the network, and user's computer. Email addresses are also standardized with the employee's surname and first initial. In the instance where there are users with same surname and initial, the user's full name may be used as an email address. The password that an employee uses to log onto the network will be applied to access the employees email account and internet application.
- (12) The Mayor, The Speaker, The Chief Whip, Full Time Councillors, interns, and temporary appointed contractors will be issued with surnames and passwords, which will be operative until their service is terminated
- (13) Passwords must not contain the user's entire parts of the user Surname or employee number.
- (14) Passwords must contain characters from three of the following five categories:
 - (i) Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
 - (ii) Lowercase characters of European languages (a through z, with sharps, with Greek and Cyrillic characters)
 - (iii) Base 10 digits (0 through 9)

- (iv) Any Unicode character that is categorized as an alphabetic character but is not upper or lowercase. This includes Unicode Characters from Asian languages
- (v) Non alphanumeric character: ~!@#%&* -+= '(){}:;''<.>./

- (15) Passwords must never be written down on a piece of paper.
- (16) Never share passwords with anyone
- (17) Use different passwords for all user accounts
- (18) Passwords should be changed every 30 days
- (19) Officials shall not share their passwords with other officials
- (20) Keep your passwords safe and secret.
- (21) No official is allowed to show their passwords to GGITO official for many reasons.

9.2 Remote Access Connections

- (1) A remote access connection is only allowed for server access and authorization must be granted by IT Manager and every activity will be monitored and changes recorded.

9.3 Server Access

- (1) Physical access to servers must be limited to GGITO officials and all changes to servers must be made in accordance with the change management policies and procedure manuals
- (2) All users with administrative access must be documented.
- (3) GGITO officials will use their login credentials to log on the servers at all times.
- (4) No officials will use the server room as an office including GGITO officials. GGITO offices will be in close proximity to the server room.

9.4 Client Data Access

- (1) User Data folders must have permissions enabled and only the owner of the folder and files and Administrators should be allowed to these folders.

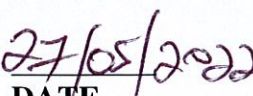
10. POLICY REVIEW

The policy shall be reviewed as and when necessary.

SIGNED BY:

MAYOR: CLLR ZITHA T


SIGNATURE


DATE

COUNCIL RESOLUTION: CR133 – 27/05/22 SP