ACCESS TO IT NETWORK POLICY AND PROCEDURES

MUNISIPALITEIT
RICHTERSVELD
MUNICIPALITY

Approved Date: 29 August 2017	**Council Resolution Nr: RVN 020/08/2017**
Effective Date: 01 September 2017	**Review Date: 30 June 2018**

1. PURPOSE

To enable the municipality to control changes and additions and access to the Information Technology environment, the completion of a change request form is required.

E-mail is a very powerful tool in business and facilitates the effective communication between Individuals on a computer network. However, if it is not used in the correct manner, networks, Systems and many other services could be halted as a result of issues like "flooding of networks".

2. SCOPE

This document covers the entire municipality's requirement with regards access to any IT equipment, application and/or electronic mail connected to the local LAN and/or WAN and is applicable to all PC users connected to the network.

3. ASSOCIATED DOCUMENTS

All municipal security and standards documents on hardware and software, Internet, Email Acceptable Usage Policies and Network Security policy

4. DEFINITIONS

E-mail - Electronic Mail on a computer network
Internet - The global information "highway"
Internet mail - E-mail via the Internet
LAN - Local Area network: the connection between PC's in offices and the local servers/main Computer that enables printing and file serving.
WAN – Wide Area Network: the connection/s between the different municipal sites that enable communication and services between the organisational Units.

5. APPLICATION

Any application (E-mail, Network, Promun, IMIS, Internet and/or other Business applications) will only be available to users connected to the municipal network. In order to be connected to the municipal network, the relevant user must:

- Fill out a User Access form
- Obtain approval from his/her direct manager (supervisor) and Director for the relevant authority and access to files and data.
- Forward approved form to the IT Department for approval & implementation.

- IT will open ticket according to removal form, once completed, signed off and ticket closed.

6. USER DEREGISTRATION

Access rights of users who have left the company should immediately be removed, procedure in place:

- User must complete access Removal form signed by his/her direct manager (supervisor) and Director.
- IT will open ticket according to removal form, once completed, signed off and ticket closed.

7. REVIEW OF USER ACCESS RIGHTS

Review of user access rights is necessary to maintain effective control access to data and information services. User's access rights should be reviewed as follows:

- As need arises.
- After any changes such as promotion, demotion, termination.
- Transfer from division to another within the same company.

8. DEVIATIONS

In the event of a deviation from the above policy, a formal request is to be made via your manager to the IT Manager of the site.

These approved forms of deviations are to be strictly controlled by the IT Department.

9. UNAUTHORISED ACTIVITIES

If any user is found guilty of deviations from the above policy without the approval from management, it will be seen in a serious light. Action will be taken against such individuals and may take the form of:

- disciplinary action
- removal from the system
- access denied to network

10. GENERAL

On resignation of any municipality employee, a notification must be sent by HR to the IT Department by filling in a User Access Removal form in order to delete the relevant user profiles from the LAN and other relevant computer systems.

A copy of the notification is kept by IT for record purposes and future reference.

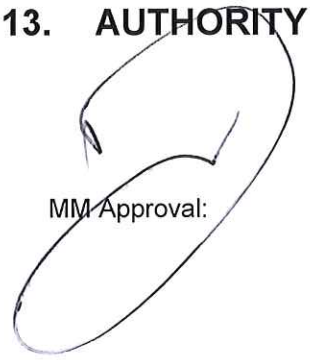
11. RESPONSIBILITY

All Information Technology employees are responsible for maintaining the confidentiality and privacy of the data under our administrative control with our information technology systems and providing access only to those who have rights to this information Examples of confidential or private data may include, but are not limited to, employee information, financial data, assets, communications, personal data storage, network transaction contents, authorization codes/passwords for access to system etc. Information Technology will ensure on upon resignation of employee, that the data of the user is backed up if needed and hard drive erased, before returned to assets.

12. POLICY REVIEWS

The Policies will be reviewed on an annual basis ensuring that it will be passed by the council.

13. AUTHORITY



MM Approval: Date:

Council Approval: Date: