

---

# MATATIELE LOCAL MUNICIPALITY

## NETWORK SECURITY POLICY

---



## INDEX

	<u>Page</u>
<u>PART 1</u> : OBJECTIVE	3
<u>PART 2</u> : ACCESS CONTROL	3
2.1 General	3
2.2 Physical Access to Terminals	3
2.3 Access to the IT System	4
2.4 Access to Specific Commands, Transactions, Programmes and Data within the System	4
2.5 User Codes and Passwords	5
2.6 Wireless Access Point Security	6
<u>PART 3</u> : SECURITY	6
<u>PART 4</u> : VIRUS PREVENTION	7
<u>PART 5</u> : USER RESPONSIBILITY	7

## 1. OBJECTIVE

The objective of the policy is to define the guidelines to be instituted to ensure the security of the municipality's Information technology systems and accompanying data.

## 2. ACCESS CONTROL

### 2.1. General

Access control is necessary to restrict unauthorised users access to any portion of the IT network or to any particular component of the system. It is therefore necessary that a bona fide user, in order to gain access, must first be authorised, that is, the access of such user to the system must be properly authenticated.

Access to the IT network comprises three steps:

- physical access to a terminal;
- access to the system; and
- access to specific commands, transactions, programmes and data within the system.

### 2.2. Physical Access to Terminals

After a bona fide user has switched on his or her computer, such user must immediately enter the required code before the computer will boot up. Thereafter the user must enter that particular computer's unique password to gain further access (see 2.5 below).

Employees with portable (laptop) computers must take reasonable precautions. When out of the office, the computer should always be under direct control of the employee or out of sight in a secure location. When in

the office, laptop computers must be locked up overnight and at weekends.

### 2.3. Access to the IT System

Access to individual software packages shall be limited to the officials whose responsibilities require them to make use of the packages concerned. The job descriptions of these officials shall be supplied to the CIO by each head of department concerned, and the CIO shall verify the need of the official in question, in terms of the job description provided, to have access to any particular package.

The CIO will provide agency/temporary/contract and freelance staff with access to computers and the municipality's computer systems for the sole purpose of fulfilling their contractual role with the municipality.

Before any bona fide user can gain access to any of these packages, such user must first enter a unique user code and password (see 2.5 below).

### 2.4. Access to Specific Commands, Transactions, Programmes and Data within the System

The financial management package used on the IT network is Abakus. This package allows access to be limited to various commands, transactions, programmes and data through the setting of access level priorities. The higher the priority, the higher the level of access which may be obtained. The CIO shall set such access level priorities in accordance with the job descriptions of the officials concerned and to comply with the specific further requirements of the relevant supervisors in the Finance Department.

Access level priorities shall be set out in writing by the CIO, and only the CIO shall be authorised to effect any amendments to such priorities.

## 2.5. User Codes and Passwords

All officials to whom user codes and passwords have been allocated, must ensure that these codes and passwords are properly safeguarded. Under no circumstances may employees share any user code or password with colleagues. Any failure to comply with this requirement shall entail prompt disciplinary action being taken against any employees who share their codes or who use codes allocated to other users.

The CIO shall have a list available of all user codes and passwords, and shall ensure that this list is kept in a secure place with other IT related securities.

The CIO shall ensure that all user codes and passwords are changed on a quarterly basis.

The following data shall not be considered as acceptable user codes and passwords:

- a user's name and date of birth;
- the name of a user's partner and such partner's date of birth;
- the names and dates of birth of any family members of the user; and
- nicknames and the like.

To be acceptable, user codes and passwords shall consist of the following:

- at least six digits;
- a combination of alpha and numeric characters; and
- a combination of higher and lower case alpha characters.

The CIO shall ensure that access privileges of any dismissed, resigned, retired or transferred officials are immediately revoked.

## 2.6. Wireless Access Point Security

All wireless access points should be secured with a password and the SSID broadcast should be set to hidden to prevent unwanted access. When access is required for a person from outside, a guest account can be used to allow them access to the internet or whatever level of system access is required for them.

## 3. SECURITY

Security arrangements should include the following:

- 3.1. Any official who obtains a password or user code (ID) which allows access to the internet and/or the municipality's IT network shall keep such password and code confidential, except if any occasion arises where any authorised technical support official requires knowledge of such password or code in order to solve a computer-related problem. Whenever a password is revealed to the system's administrator or user support, it should be subsequently changed to prevent that user's information be accessed without consent.
- 3.2. As set out in 2.5 above, the present policy strictly prohibits the sharing of user codes or passwords between employees. Furthermore, logging onto the IT network or internet with one's personal code and password, and then allowing another user to use or work on the internet or network, shall be viewed as an attempt to bypass official security procedures, and is strictly prohibited.
- 3.3. Each terminal should have a password on the local administrator account, as this account can be used to gain access to the user's files on the machine without consent. This should also be changed on a six monthly basis and the password should only be known to the systems administrator or user support.

- 3.4. Only encryption software supplied by the CIO for purposes of safeguarding sensitive or confidential business information may be used. People who use encryption on files stored on a municipality-owned computer must provide the CIO with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

#### 4. VIRUS PREVENTION

- 4.1. An antivirus software package must be loaded onto the server and user terminals (when allowed individual access), which antivirus software must have the ability to update via the internet. The software must be able to scan for viruses, Trojans, malware and spyware, as well as remove or advise on removal of any infection that may occur.
- 4.2. All emails sent and received by the company should be scanned for viruses and potentially dangerous content, such as executables (.exe), batch files (.bat) or any file that could potentially harm the computer or the network.
- 4.3. Any user found disabling or to have disabled the antivirus would receive a formal warning as this creates a potential security threat for the network.

#### 5. USER RESPONSIBILITY

- 5.1. Every authorised user shall sign all security and confidentiality agreements required by the CIO before attempting to gain access to the internet and/or the IT network, as provided for in the Information Technology Policy.
- 5.2. Prompt disciplinary action shall be instituted against any official who attempts to disable, defeat or circumvent any firewall, proxy, internet address screening programme and any other security systems installed by the CIO and System Administrator or by the municipality's IT suppliers to assure the safety and security of the municipality's IT network.