

Mobile Devices Policy

1. Purpose

This policy is intended to manage the risks of mobile computing by:

1. Ensuring the Municipality mobile computing assets are appropriately procured and reasonably or fairly allocated and managed
2. Implementing a uniform and consistent approach to security issues associated with mobile computing devices
3. Providing guidelines that assist protection of the confidentiality, availability and integrity of municipality information while stored, transmitted or processed using mobile computing devices and
4. Ensuring that users of mobile computing are aware of their responsibilities.

2. Scope



This policy covers mobile computing devices used for municipality purposes including (but not limited to):

1. Laptops/notebooks/netbooks.
2. Tablet devices (e.g. Apple IPad, Samsung Galaxy, etc.).
3. Smartphones and mobile 3G Modems

3. Allocation and qualifying for Mobile device

The following devices are mobile devices:

Device name/type	Basic Function	Extra-enabled function
Laptop	Offers ability to do productive computing, and ability to run all programs	<ol style="list-style-type: none"> 1. Complete Computing device 2. Ability to use LAN internet and 3G SIM Card internet
Tablet	<ol style="list-style-type: none"> 1. Offers most portability and comfort compared to laptops, they are mostly 10 inches or less in size 2. Internet Access enabled 3. Wi-Fi Access enabled 4. Wi-Fi Hotspot (Ability to share internet with laptops) 	<ol style="list-style-type: none"> 1. Communication tool (audio calls making and receiving – .i.e Samsung galaxies)

Initiated By:	Management Representative		Issue Date:	
Authorised By:	Municipal Manager		Revision No:	
Issuing Office:	Mohokare Local Municipality – Zastron		Revision Date:	7 October 2016
Document No:	Policies & Procedures Manual	Controlled Copy	Version No: 0	Page 1 of 3

	or other devices)	
Smartphones	1. Communication tool(audio and video calls making and receiving)	1. Internet Access enabled 2. Wi-Fi Access enabled 3. Wi-Fi Hotspot (Ability to share internet with laptops or other devices)
3G SIM Card Modems	1. Internet Access	

It is standard for the municipality to provide one computer device (either an onsite desktop personal computer or a laptop), based on the employee's business need by role/function.

Only the municipal manager, and high-level management such as directors, may receive a choice of three of the mobile devices as indicated in the above table, due to the following reasons:

- a) By default, this management may at all times be required to do their task after hours of work
- b) This management is as equally mobile as they are office-based as they carry out their tasks
- c) They need a back-up device for internet access

On exceptional cases and where motivation is given, an employee may receive a secondary device for other purpose such internet access and calls making and receiving.

The head of department should provide a motivation as to why an employee deserves to receive an additional mobile device for internet access.



The motivation should at the least prove the following reasons factually:

- 1. The employer's need to contact the employee at all times for work-related emergencies, outside of the employee's normal work day.
- 2. The employer's requirement that the employee be available to conduct municipality business when the employee is away from the office.
- 3. The motivation should indicate that the essential need to the employee's job duties to have access to the internet-related resources that cannot reasonably be fulfilled with municipality network resources

Furthermore, the above motivation should be documented well enough, with respect to the duties and responsibilities of each employee.

If an employee changes, job title, due to him or her being promoted, demoted, or transferred to another position, the mobile device should be returned and new motivation be provided in line with the new position.

Mobile computing devices must not be transferred from the original allocated employee to another employee, the devices must be returned to the IT Unit, for asset tracking, security and future re-allocation.

Initiated By:	Management Representative		Issue Date:	
Authorised By:	Municipal Manager		Revision No:	
Issuing Office:	Mohokare Local Municipality – Zastron		Revision Date:	7 October 2016
Document No:	Policies & Procedures Manual	Controlled Copy	Version No: 0	Page 2 of 3

NB:

- a) The office-based Internet facility is the primary tool to be used by employees to complete their day-to-day functions, and 3G Internet is a secondary tool
- b) An occasional need to access the internet after hours, does not necessarily justify the need to receive a 3G SIM Card/or Modem
- c) Employees are encouraged to complete tasks that require internet access while they at the office and can use the office-based internet.
- d) One 3G SIM Card and Modem is available for one (1) day lease on emergency need for other employees, and is leased on first-come first-serve bases.



4. Employee Responsibilities

Employee shall at all times, take total responsibility of the device provided to them by the municipality, and shall therefore ensure that:

- Access to information contained on the mobile device will be protected by a minimum of a password OR pin and that these are not saved in device, type/written onto a paper and left in the carry bag.
- No unauthorised user is allowed to use the mobile device. This includes lending the device or handing it over for physical possession of the device to an unauthorised party.
- When the municipality's network is accessed from remote areas (outside) that the necessary security software that will establish secure communication to the municipality's security systems is utilised.
- Necessary caution will be exercised when working on municipality related information in public areas as external parties could easily read information off screens.
- Ensure when staying in hotels to make certain that the device is locked in the hotel's safekeeping and not left unattended in the hotel room.
- In the event of a mobile device being stolen, immediately report the theft to the immediate supervisor, security manager, and the IT Unit to arrange for all security access to be suspended.
- An employee is totally responsible for safe-keeping of the mobile devices at all times.

5. Policy Review

This policy shall be reviewed annually.

Initiated By:	Management Representative		Issue Date:	
Authorised By:	Municipal Manager		Revision No:	
Issuing Office:	Mohokare Local Municipality – Zastron		Revision Date:	7 October 2016
Document No:	Policies & Procedures Manual	Controlled Copy	Version No: 0	Page 3 of 3