Laptop Policy

& Guidance

MATJHABENG LOCAL MUNICIPALITY

LAPTOP POLICY & GUIDANCE

DOCUMENT CONTROL

DOCUMENT DETAILS

Author	PLM Rakotsoane
Company Name	Matjhabeng Local Municipality
Division Name	Information & Communication Technology
Document Name	Laptop Policy & Guidance
Version Date	05/03/2019
Effective Date	
Review Date	

Stakeholder Sign–off

Name	**Position**	**Signature**	**Date**
PLM RAKOTSOANE	ICT Manager		
TUMELO MAKOFANE	Executive Director SSS		
THABISO TSOAELI	Municipal Manager		

Security Sign-off

Name	**Position**	**Signature**	**Date**
PLM RAKOTSOANE	Acting ICT Manager		

1. PURPOSE

The purpose of this policy is thus to provide fairness in the procurement and allocation of notebook or laptop personal computers for use by employees as a work facility, to protect the confidentiality, integrity and availability of Matjhabeng Municipality's information by controlling access to its laptops and to provide guidelines for the use of laptops.

2. SCOPE

The scope of this policy applies to:

- Any laptop owned by The Matjhabeng; and
- Any person authorised by The Matjhabeng to use the laptop.

3. POLICY

3.1. Policy Statement

The Matjhabeng's information system resources are assets important to The Matjhabeng's business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. At any given time, some of The Matjhabeng's information resources will be held on, or will be accessible from, laptops, of which a proportion will regularly be removed from The Matjhabeng's premises. It is The Matjhabeng's policy that appropriate access control measures are implemented to protect its information system resources, as held on or accessible from laptops, against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

3.2. Policy Objectives

The objectives of this policy with regard to the protection of information system resources as held on or accessible from laptops against unauthorised access are to:

- Minimize the threat of accidental, unauthorised or inappropriate access to electronic information owned by The Matjhabeng or temporarily entrusted to it;
- Minimize The Matjhabeng's network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources;
- Minimize reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality; and

- Minimize the risk of physical loss of the laptop.

3.3. Policy Overview

The Matjhabeng information system resources, as held on or accessible from laptops, are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Adequate precautions are required to prevent and detect unwanted access. Users should be made aware of the dangers of unauthorised access, and managers should, where appropriate, introduce special controls to detect or prevent such access.

3.4. Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an on-going basis by The Matjhabeng ICT department. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from The Matjhabeng Intranet or other relevant communication media on an on-going basis and accept the terms and conditions contained therein.

4. POLICY REQUIREMENTS

The Matjhabeng's information system resources, as held on or accessible from laptops, shall be appropriately protected to prevent unauthorised access.

4.1. General

- Laptops are an essential business tool, but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside of The Matjhabeng's premises increases the threats from people who do not work for Matjhabeng Municipality and may not have its interests at heart.
- Laptops are especially vulnerable to physical damage or loss, and theft – either for resale or for the information they contain.
- If a laptop or any of its accessories is lost due to outright negligence, a staff member shall make good the loss financially. The current method of recovering the lost to the equipment utilized by Procurement

division will be used or payment arrangements should be done with Salaries division with the assistance of ICT for the repayable amount.

- The impacts of breaches of security involving laptops include not just the replacement value of the hardware but also the value of any data on them, or accessible through them. Information is a vital asset. The Matjhabeng depends very heavily on its computer systems to provide complete and accurate business information when and where required. The impacts of unauthorised access to or modification of, critical or sensitive data will usually far outweigh the cost of the equipment itself.

4.2. Access to on/off-line Information

The following guidelines must be observed.

- The physical security of any laptop being used by you is your personal responsibility, so you must take all reasonable precautions. Be sensible and stay alert to the risks.

- Keep your laptop within your possession and within sight whenever possible, especially in busy public places such as airports, railway stations or restaurants.

- Lock the laptop with a defcon cable while in the office; lock it away out of sight when you are not using it. Never leave a laptop visibly unattended in a vehicle. If necessary, lock it out of sight in the boot and ensure that your car doors are locked.

- A space has been reserved on a file server for a laptop user to periodically back/synchronize the data or documents on his or her PC. The onus to backup data and documents rests with the user.

- The data or documents on any personal computer are, in the first instance, the property of MLM. Archive regulations therefore apply to these data and documents.

- When you are engaged in a meeting and you leave your desk or table for coffee or tea break or lunch, log off from the operating system, and always ensure that your screen is locked every 10 minutes or so of keyboard inactivity, to prevent access to your data on your PC by other persons.

- An employee to whom a laptop has been allocated or provided is responsible for then safety and custodianship of the laptop in the office and outside the office. If employee lost a laptop more than once, a replacement of that will be a PC, this is to protect Municipal information.

- Carry and store the laptop in a padded laptop bag or strong briefcase to reduce the chance of accidental damage.

- The ICT helpdesk maintain records of the make, model, serial number and The Matjhabeng's asset label of your laptop, then do not transfer it to the next person without ICT consent. If it is lost or stolen, you can contact them for this information. It is your responsibility to notify the Police immediately and inform the ICT helpdesk as soon as is reasonably practicable.

- Viruses are a major threat to the Organization and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software will update automatically every time you connect to the Network. If you have reason to believe that this is not happening, please contact the ICT helpdesk for advice.

- Avoid opening any unexplained email attachments.

- Virus scans normally happen automatically but the ICT helpdesk can tell you how to initiate manual scans if you wish to be certain.

- Respond immediately to any virus warning message on your computer, or, if you suspect a virus (e.g. by unusual file activity,) please contact the ICT helpdesk at 3422. Refer to "Anti-Virus" section of Malicious Code Policy & Guidance for more information.

- Laptops must have correctly-configured firewall software installed and switched-on. If you have any reason to believe that this is not the case, please contact the ICT helpdesk at 3422.

- You are personally accountable for all network and systems accessed under your user ID, so keep your log in details secret.

- Laptops are provided for official use by authorised employees. Do not loan your laptop or allow it to be used by others such as family and friends.

- A laptop user shall not use the laptop for private financial gain.

- In particular, laptop control is defined as the means of ensuring that the variable subset of The Matjhabeng’s electronic information resources which is held on or accessible from laptops is available only to persons authorised to view or process that information in accordance with pre-determined rules.

- Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine, also avoid leaving your laptop in the office when you knock off.

- The contents of a laptop screen are easily observed by someone sitting in close proximity. Please ensure that no sensitive or critical information can be viewed by an unauthorised person when using the laptop in a location away from The Matjhabeng’s premises (e.g. a restaurant).

- Ensure that when you are connecting to The Matjhabeng network (LAN) that you do not have your wireless or 3G connections enabled as this could allow a bridging from external networks into our corporate network.

- Upon departure from service in the municipality, a laptop must be returned to the ICT Manager. It is the employee’s responsibility to obtain an acknowledgement of receipt.

- Both the supervisor and an employee shall be held personally liable for any loss incurred by the Department for a notebook that has not been deposited with ICT upon departure, this failure will impact an employee final remuneration package. An employee may purchase a laptop at fair market value on their departure. Fair market value is designated as 25% of the purchase amount if a laptop has already exceeded its lifespan of 3 years. A purchase is subject to Municipal’s approval.

- ICT remain responsible for recommending the new technologies, giving the specifications and the model of the laptops should be procured. Any employee wishes to deviate will be liable for additional costs whereas the laptop will remain Municipal property. Only executive managers/super systems user (**EXCO level**) will be able to deviate from standard users' specifications but only up to R30 000, executive manager/super systems user wishes to deviate will be liable for additional costs whereas the laptop will remain Municipal property.

- This Policy may be used with Laptops terms of Use.

4.4. Policies

Laptops are subject to The Matjhabeng's full range of policies. Please ensure that you are familiar with them.
A laptop being used in an external location is no different from the point of view of applicability of policies from a PC being used within The Matjhabeng's premises.

4.5. Backups

If file content is being changed and is not transferred regularly to the corporate network, it is your responsibility you must take your own backups of data on your laptop on a regular basis.
It is your responsibility to take regular off-line backups to a suitable storage (**U drive; OneDrive**). Backups must be encrypted and physically secured.

4.6. Health and Safety Aspects of Using Laptops

Laptops normally have smaller keyboards, displays and pointing devices than desktop systems.
Because these may be less comfortable to use, there may be an increased risk of repetitive strain
injury. If you experience any symptoms whatsoever which might be caused by laptop use, please
discontinue using it immediately and report the matter to the Health and Safety Department.
Do not balance the laptop on your knees as this can cause back injury. Wherever possible, place
the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it.

4.7. Reporting Security Incidents

All security incidents, including actual or potential unauthorised access to the Matjhabeng's information systems via laptop, should be reported immediately to the ICT Manager.

4.8. User Awareness

Users shall be made aware of their responsibilities in the prevention of unauthorised access to Matjhabeng information resources via laptop, including, but not limited to:

- That no equipment is left logged-in without the protection of an activated password protected screensaver;
- The need to be aware of this Policy and all its provisions.

5. STAFF MEMBERS TO WHOM LAPTOPS MAY BE PROVIDED

- All below laptop applicants SHOULD be in possession of the vehicle. Proof of vehicle ownership should be attached on the application.
  - The Mayor of Matjhabeng Municipality.
  - The Speaker of Matjhabeng municipality.
  - The Chief Whip of Matjhabeng municipality.
  - Members of Mayoral Committee of Matjhabeng Municipality.
  - Section 57 Managers.
  - The Senior Managers of Matjhabeng Municipality.
  - Managers of Matjhabeng Municipality.
  - Personal Assistants
  - Work study officers
  - Project managers.
  - Internal Auditors
  - Technical support staff, for example, information Technology Officers/technicians.
  - Staff members whose duties include Departmental research or
  - Anyone who is a member of legislated Council Meeting.

6. INSURANCE

- Laptops are thus insured.
- Members of staff should take note that household insurance does not cover employer property located in the house of a staff member.
- Members of the staff should report a loss/theft/damage incident to ICT as soon as practical. ICT will give out equipment details then the members of the staff should report loss/theft to SAPS and acquire case number and affidavit for insurance claims.

- Members of staff are either liable for payment of excess fee for the laptop replacement or replacement costs in case the insurance do not replace an item and it's proven that it's due to negligence.
- Conditions leading to insurance claims rejections:
  - Late claims submission;
  - Jam locking incidents
  - Non-Forcible entry (***Stolen without breaking doors, windows or walls)***

7. SOFTWARE LICENSING

Only software that has been licensed by the MLM may be loaded on a laptop.

8. SECURITY GATE PASS CONTROL

Laptops shall be checked out and checked in with security at entrance gates. Gate security shall record the make, model and departmental inventory numbers in a register

9. DISCIPLINARY PROCESS

The Matjhabeng reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with The Matjhabeng's Rules and Disciplinary Code as amended from time to time. Disciplinary action may ultimately lead to dismissal.

10. DEVIATIONS FROM POLICY

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation to or non-compliance with this policy shall be reported to the ICT Manager.

11. CONCLUSION

- This policy is short, and this should enable staff members to commit to memory the stipulations contained herein. By making use of a laptop, a staff member implicitly acknowledges this policy and agrees to abide by the policy in its entirety.
- This policy is subject to change from time to time.