the dr&pw

Department:
Roads and Public Works
NORTHERN CAPE PROVINCE
REPUBLIC OF SOUTH AFRICA

DEPARTMENTAL POLICY ON UTILIZATION OF LAPTOP COMPUTERS

Version 2

(Reviewed in March 2015)

TABLE OF CONTENTS

Contents Page

1. DEFINITIONS

I.T.	Information Technology.
Laptop computer	A personal computer designed for mobile use and small light enough to sit on a person's lap while in use. A laptop integrates most of the typical components of a desktop computer, including a display, a keyboard, a pointing device (a touchpad, also known as a trackpad, and/or a pointing stick),speakers, and often including a battery, into a single small and light unit.
Programme Managers	Means Senior Managers appointed by the Accounting Officer to manage a specific programme
Responsibility Manager	Means Managers responsible for a specific unit
Write-offs	Means equipment that are no longer functional.

2. INTRODUCTION

2.1. This laptop policy is a document that states in writing the rules and practices to be conformed to at all times by the employees of the department in the allocation, use and in order to ensure the safety of laptops issued to them and the data stored in the machines. This policy is a formal document to be read by employees.

2.2. A laptop is intended for use by departmental officials as a productivity tool and communication. It is not intended as a replacement for any computers that may be owned personally. Use of the laptop for personal purposes should be within the standards of good judgment and common sense and as required through the terms and conditions of applicable software license agreements.

3. REGULATORY FRAMEWORK

3.1. In terms of the Public Finance Management Act no.1 of 1999 (as amended by Act no 29 of 1999 the Accounting Officer (AO) is responsible for:

3.2. The effective efficient and transparent use of the resources of the Department (Sections 38(1)(b));

3.3. The management, including the safeguarding and maintenance of assets of the Department (Section 38 d)(l));

3.4. May not commit the Department to a liability for which money has not been appropriated.8(2).

3.5. In terms of section 45 an official in the department-

a) must ensure that the system of financial management and internal control established for that department, trading entity or constitutional institution is carried out within the area of responsibility of that official (Section 45(a));

b) is responsible for the effective, efficient, economical and transparent use of financial and other resources within that official's area of responsibility (Section 45(b));

c) is responsible for the management, including the safeguarding, of the assets and the management of the liabilities within that official's area of responsibility (Section 45(e).

3.6. Treasury Regulations March 2005 Chapter 10.1.1 and 10.1.2 (Asset Management)

4. OBJECTIVE

4.1. This policy is to provide support services and management of the department through managerial and administrative guidance.

4.2. The objective of this policy is to ensure that:

a) All laptop computers allocated are essential for an employee to perform his/her duties for which he/she was appointed.

b) Allocation of all laptop computers is authorised.

c) The validity of allocations of laptop computers.

d) Guidelines are provided for the allocation and utilisation of pool laptop computers within the Department.

e) Employees are made aware of their responsibilities towards the safeguarding of the laptop computers in their possession.

5. PRINCIPLES, VALUES AND PHILOSOPHY

This policy is intended to reflect the department's commitment to the principles, goals and ideals described in the department vision and core values.

6. SCOPE AND APPLICABILITY

6.1. This policy covers the issuing, usage and safeguarding of laptops by permanent Departmental staff where the regular use of a laptop is necessary or useful to meet the requirements of the job.

6.2. The Departmental officials who qualify for the usage of official laptops as provided for in this policy are the following:

a) Head of Department

b) Senior Management Services Members

c) Deputy Directors.

d) Personal Assistants Head of Department (HOD).

e) Any other official recommended by the relevant Programme Manager and approved by the Head of Department.

7. PROCEDURES

7.1. New applications

If the official does not quali fy in line with provision 6 for a laptop the relevant Programme Managers shall submit a request to the AO for a laptop. The AO will consider all requests for allocations on the basis of motivation, which shall be in accordance with the conditions as specified in below.

Qualifying criteria and information necessary to consider new applications for departmental cellular contract phone:

a) a laptop must be vital and necessary for the execution of official duties;

b) the detailed reasons and motivation for the request must be furnished;

c) details of other means of completing the work shall be considered;

d) financial implications, including quotations from three service providers, total cost and availability of funds in the directorate's budget; and;

If the request is approved by the AO the acquisition of the laptop must be done via the normal Supply Chain Management processes.

7.2. Official resigning or termination of service

When an official resigns or services are terminate for whatever reason the laptop must be returned to Asset Management on the last day of service. If not the official will also be held responsible for the replacement of the laptop not returned.

7.3. Withdrawal of allocated laptops

In the following circumstances allocated computers can be withdrawn if it is in the best interest of the Department of Roads and Public Works to do so:

a) If the official failed to take adequate steps to safeguard the laptop computer against damage and loss at all times.

b) Use of the laptop for any other reason that allocation was intended for.

7.4. Appropriate Use of laptops

a) The Department does not tolerate inappropriate use of any company property. Use your laptop only for business purposes. Offensive, pornographic, racist or abusive content found on departmental laptops will be referred as necessary under The Departments disciplinary proceedings. Serious offences will be reported as necessary to the police.

b) Your email should be filtered for spam. If you receive any inappropriate material by email delete it immediately. If persistent, report to the helpdesk for investigation.

c) Only visit Web sites you know and trust.

d) The departments network is monitored for inappropriate use. Offenders will be reported to their line managers for further disciplinary action.

7.5. Use, safeguarding and safekeeping of laptops

a) The laptop serial number, make and model should be recorded prior to issue on an acknowledgement of a receipt form..

b) The laptop information must be recorded on the official's inventory list that includes the laptop/ computer equipment.

c) The inventory register as well as the acknowledgment of receipt form at IT, must be completed and signed by the official undertaking responsibility for the use of the laptop.

d) If the laptop is stolen or lost this should be reported to the South African Police within 48 hours and the SCM unit, Asset Management, of the Department immediately in writing.

e) There must be supporting documentation to the above.

f) Once the laptop is lost/damage or stolen, the department will replace the laptop as soon as possible while the investigation is being undertaken.

g) In cases where laptop are lost through the negligence of the official, the cost of replacement will be recovered from the official.

- Negligence constitutes the following:
  - disappearance from place of residence, unless forced entry can be proved;
  - leaving an office unlocked;
  - leaving a laptop exposed in a vehicle, e.g. in the cabin, which leads to it being stolen/damaged.

h) All laptops to be supplied with a lock, e.g. legion lock in order to assist in safeguarding laptops. Where locks are issued, users are expected to:

- Lock equipment at all times in areas open to the public, even when in use.
- Lock equipment while travelling whenever possible.
- Lock equipment at home when not in use.
- In recognition that a lock only reduces the risk of laptop theft, the department expects all line managers and the helpdesk to reinforce the need for users to be aware of the risk of theft and to offer advice including the following:

  - Don't depend on a lock as the only security.
  - Always lock out of sight if not in use.

- Never leave a laptop logged on to networks, email and Web sites. Always shut down or activate a password-protected screensaver.

7.6. Disposal of laptops

a) The disposal of laptop equipment must be by recommendation of the Departmental Disposal Committee. Laptop equipment should be disposed of according to asset disposal policy.

b) The final authorization for the disposal of the laptop equipment is the responsibility of the Accounting Officer or a duly delegated official.

8. ROLES AND RESPONSIBILITIES

8.1. Programme managers are responsible for the implementation of the policy.

8.2. Financial Accounting: Division - Theft and Losses are responsible for the safeguarding and maintenance of the assets

8.3. Ownership and possession of laptop computers

a) Laptop computers allocated to officials of the Department who qualify for this benefit, remain the property of the Department.

b) The officials are responsible for the safekeeping of these laptops, to ensure that they function effectively. The onus is on the official to ensure that the laptop computer is protected against theft and damage.

c) The officials who are allocated with laptop computers acknowledge that the computer is a work tool and that they will therefore use it to the benefit of the Department and for work purposes only.

8.4. Laptop User General Responsibilities

a) General

- Don't leave laptops unattended and always lock.
- Don't allow anyone else to use your laptop
- If left at work overnight, lock out of sight.
- Choose an ordinary looking briefcase or non-traditional laptop carry bag, perhaps a back pack type, as bags that obviously contain computers are an easily identifiable target for the casual thief.

b) At Home

- Always store inside your home, never leave in the car and keep where it cannot be easily seen from outside. Ideally, keep locked in a cupboard or strong drawer.
- When it is not possible to lock away, use your supplied T-bar lock attaching to either an immoveable object or to something that is difficult or heavy to carry.
- Do not allow any use that is not authorised by the department.
- Only use in an office-like environment with table and chair. Do not be tempted to use near water.
- Only connect to approved or known wireless networks. Ideally use your encrypted domestic connection if available.

c) In the Car

- Your laptop will be safer if it is not left in the car at all.
- If absolutely necessary, lock out of sight in the boot.
- If you expect to leave your laptop in the car regularly, speak to the helpdesk and ask about additional security measures. An in-car vault or separate lock to leave in your boot which can be locked to the spare wheel may be offered.

- Consider the overall security of the vehicle in terms of the location, time of day and duration of your stay when parking.
- While the vehicle is in motion, your laptop should be stored in its carry bag. Ideally secure in the boot; a heavy item such as a laptop can become a hazard to vehicle occupants in an accident.
- Only connect to approved or known wireless networks.

d) Public Transport and Public Places

- Laptops are particularly vulnerable to theft and loss while using public transport. Be vigilant.
- Do not use your laptop while travelling unless necessary. Even then, consider the location you choose with care. Ensure you are not easily overlooked and never open documents or communications that are of a commercially or personally sensitive nature while in a public place.
- Never leave unattended and never allow anyone else to use your laptop.
- Be aware of your surroundings. Ensure you are not exposing yourself or the laptop to opportunistic theft.
- Always use your T-bar cable lock, even when working, to avoid the laptop being easily snatched.
- Only connect to approved or known wireless networks.

e) Hotel, Conference and Meeting Rooms

- Avoid leaving laptops in hotel rooms. Use the hotel safe and get a receipt. If absolutely necessary, use your T-bar lock.
- In conference and meeting rooms, use your T-bar lock. It is good practice to do this even when working so that it isn't later forgotten at a coffee break. For longer breaks, shut down and take your laptop with you.

8.5. Laptop user data protection responsibility

a) Always use encryption software approved and supplied by the department.

b) Choose a password that is unique to your data-encryption key; make it long, random and complicated to guess.

c) Do not give your network password or token/access device to anyone. You are responsible for all access under these codes.

d) Remember that access to your laptop can also mean access to the department's network.

e) Your laptop is the property of the department; do not lend it to anyone or otherwise permit use by anyone else, not even for a short while.

f) If you leave your laptop switched on and unattended you must activate the password protected screensaver. Ideally, never leave switched on or logged in. Log out, shut down.

8.6. Laptop user malware responsibilities

a) Malware is harmful software such as viruses and spyware. Malware on your laptop could be spread to the wider departments network or risk the security of the data on your laptop. It is important that no malware should be allowed on your computer.

b) The department provides all laptop users with pre-installed antivirus software. Make sure you know how to access and use this software. Call the helpdesk for advice if needed.

c) If you do not have regular access to the department's network then you will not receive regular antivirus updates. Make sure you log on to the company network at least once a week to allow for these important updates to take place. If this is not possible, talk to the helpdesk about ways to keep your antivirus application definitions current.

d) Always scan files for viruses. Your email is automatically scanned for you as are files from the company network, but if you are given a file on a disk, USB key or by any other means then you must first scan the disk and/or file for viruses.

e) Do not open any email attachments unless they were expected and from a trusted source. Email attachments are the number-one malware risk.

f) Do not download any software. If you need a different or more current application, contact the helpdesk for advice. Most permitted applications are updated automatically for you when you log into the departments network.

g) If you suspect a virus attack, contact the helpdesk immediately. Do not access the departments network or back up files until your laptop has been inspected.

8.7. Laptop user data recovery responsibility

a) If the worst should happen and your laptop is stolen, lost, damaged or simply fails then it is always possible to recover your data... but only up to your last backup. It is your responsibility to ensure that you make adequate backup provision.

b) When connected to the departments network, your files are automatically backed up, provided you have saved them as directed into the correct folder on your laptop.

c) You should back up at least daily when working away from the company network. Use disks or USB HDDs as necessary — always encrypt and store securely. Destroy or delete out of date backup media. Do not amass backup data.

d) Store backup data separately to your laptop.

e) Contact the helpdesk if you need advice or require specialist or additional backup.

8.8. Laptop user software responsibility

a) Your laptop is supplied with software. These are the only applications licensed for use. Do not install additional software without the express consent of the IT department.

b) Be aware of Web sites and emails guiding you to download applications. You are not authorised to do so and downloaded applications may breach company policy and expose a serious security risk.

c) If you need an additional application or update contact the helpdesk to discuss.

9. ROLES AND RESPONSIBILITIES

9.1. Programme managers are responsible for the implementation of the policy.

9.2. The Directorate Policy and Planning will monitor and evaluate compliance and impact of these guidelines by all programs and sub-programs in the Department.

9.3. Supply Chain Management is responsible for the commitment and renewal of all cellular contracts with service providers.

9.4. Management Accounting – Division Budget and Expenditure Control is responsible for the monitoring of the expenditure and budget.

9.5. Financial Accounting: Division - Theft and Losses are responsible for the safeguarding and maintenance of the assets.

10. FINANCIAL IMPLICATION

10.1. The Accounting Officer shall make a determination of needs in terms of laptop computers according to the designated Departmental Budget for a given financial year.

10.2. The Accounting Officer shall allocate all such resources (financial, human, logistical) that are necessary for laptop usage needs available to each Programme Budget in accordance with the above determination.

10.3. Directorates shall be responsible for budgeting for the implementation, monitoring and evaluation of the policy. Senior managers must take note of cost implications of the approved policy that should be borne by the respective directorates.

11. MONITORING AND EVALUATION

11.1. The Directorate Strategic Planning Management will monitor and evaluate compliance with, and the impact of, these guidelines by all programmes and sub-programmes in the Department.

11.2. The Directorate IT will monitor and evaluate compliance and impact of these guidelines by all programs and sub-programs in the Department.

11.3. The Financial Inspectorate will perform investigations with regard to compliance, regulations, policies and procedures.

12. POLICY ADOPTION AND REVIEW

12.1 This policy shall be reviewed in two (2) years from its effective date to determine its effectiveness and appropriateness. This policy may be reviewed before that time, as necessary, to reflect substantial organisational or other changes at the Department, or any change required by law.

12.2 Deviations from this policy must be approved by the Accounting Officer.

13. APPROVAL AND RECOMMENDATIONS

This policy is Approved / Not Approved

Comments:

....

....

....

....

....

HEAD OF DEPARTMENT

16/04/2015
DATE