Western Cape
Government

Social Development

Research, Population & Knowledge Management Unit
Allison.Thomas@westerncape.gov.za.
Tel: +27 21 483 4355. Fax: 086 652 0027

14 Queen Victoria Street, Cape Town, 8001

REFERENCE: 6\4\3\P
ENQUIRIES: AS. Thomas

November 26, 2012

Dr. Robert Macdonald
Acting HOD: Department of Social Development

e-Mobility Policy

1. Purpose

Approval is hereby requested from the acting HOD of the Department of Social Development's to approve the e-Mobility policy for the department.

2. Background

The province of the Western Cape has adopted e-Mobility as a mobile communication device for the province. A transversal e-mobility policy has been developed to assist departments to manage the use of these devices. Social Development has created its own e-Mobility policy as a supplement to the transversal policy to cater for its own unique environment.

3. Motivation for implementation

This policy was developed to provide governance to the usage of e-Mobility within the Department of Social Development.

4. Consultation & Communication

- Directorate: Research, Population and Knowledge Management
- C-el
- Provincial e-Mobility forum
- DSD DITCOM

Recommendation

It is hereby requested that the DSD e-Mobility policy for the Department of Social Development be approved.

Mr. G D Miller:
Director: Research, Population and Knowledge Management
Date: 2013-11-27

Supported/ ~~Not Supported~~

Ms. M. Johnson:
Chief Director: Business Planning and Strategy
Date: 27/11/13

Supported/ ~~Not Supported~~

Mr. C. Jordan
Chief Director: Social Welfare
Date: 27/11/13

Supported/ ~~Not Supported~~

Mr. M. Hewu
Chief Director: Community & Partnership Development
Date: 29/11/2013

Recommendation

It is hereby requested that the DSD e-Mobility policy for the Department of Social Development be approved.

Recommended/~~Not recommended~~

"I, the undersigned, do hereby certify that in terms of Provincial Treasury Instruction 2.2.1:

- the financial implications of the submission can be accommodated within the approved budget framework of the Department;
- the submission complies with any applicable financial statutory requirements;
- it supports the attainment of the Department's strategic objectives; and

from a financial management perspective, the submission is in order."

Comments:

....

....

....

....

Mr. J. Smith
(Chief Financial Officer)

Date : 12/12/2013

Approved/ ~~Not Approved~~

Mr. R. Macdonald
Acting HOD: Department of Social Development
Date: 13/12/13

Western Cape
Government

Social Development

DEPARTMENT OF SOCIAL DEVELOPMENT

e-MOBILITY POLICY

November 2013

6/4/3/P

1. INTRODUCTION

The Department of Social Development (Department) acknowledges and subscribes to the current eMobility policy that was approved as a transversal Western Cape Government policy by Director-General on the 4th December 2012 (see: Appendix A).

This Departmental eMobility policy does not replace the existing transversal Provincial data/eMobility policy but addresses four key points that are relevant to the Department. These points are:

- Who is entitled to an eMobility device?
- Procedure for acquisition, including VPNC
- How much CAP can be allocated to the user?
- Loss, theft and multiple use
- Disposal of eMobility devices

eMobility devices are owned by the Department and remain the property of the Department. They are made available to the employees, as a business tool. In the event of termination of service these devices must be returned to the eMobility Information Officer.

2. WHO IS ENTITLED TO THE EMOBILITY?

The Department recommends that officials who spend the majority of their working time outside office could qualify for the allocation of an eMobility device in order to access information via the Western Cape Government network provided that they meet certain predetermined criteria. Such officials could include:

- Directors
- Chief Directors
- Head Of Department
- Minister
- Regional Managers
- Corporate Managers
- Social Workers
- And any other official approved by the management

3. PROCEDURE FOR ACQUISITION, INCLUDING VPNC

Applicant

(a) Each applicant/user must have a laptop allocated to her/him as this device is generally meant to assist the official/s working outside of the head and/or regional and/or local service delivery office.

(b) An asset certificate (Form RR 032) must be attached to the eMobility application form as a confirmation that the requestor is in possession of a laptop.

(c) The applicant must furthermore include the prescribed completed VPNC form if access to applications that are not web-enabled or located behind the firewall in the VPN is required.

(d) The applicant must submit a request for eMobility using the prescribed application form via her/his supervisor and ICT budget holder (i.e. relevant SMS member).

(e) The application must be completed in full with all the required information such as Identity Number, Address and the Full names of the applicant/requestor. The supervisor and budget holder (generally an SMS member) must scrutinize the request and grant approval by signing or disapprove pending on the reasons for the decision and the availability of funds at the cost centre. All applications must be supported by the supervisor and approved by the budget holder.

Manager

(a) The eMobility is paid from the directorate/regional budget. Therefore all applications must be approved and signed by the manager and the budget holder.

(b) In case of the acting supervisor/director/regional manager, the signed application must be accompanied by the acting appointment letter.

(c) The senior manager or regional manager must also indicate the needed data cap for the particular official in each application.

eMobility Information Officer

(a) Once approved by the budget holder, the eMobility application form must be sent to the eMobility Information Officer who will ensure that all sections of the application have been correctly completed.

(b) The quality checked application is submitted by the eMobility information officer to the Department's DITCOM secretariat.

DITCOM Secretariat

(a) The eMobility information officer must assure itself that the applicant needs a data card for official purposes and that the application is motivated by the official's senior manager (in the case of a Head Office application, a Director upwards) or the Regional Manager (in the case of an applicant within a regional boundary.

(b) DITCOM secretariat must ensure that the application is completed and the RICA information on page 2 (two) of the application form is captured.

(c) The application is then referred to the DITCOM for approval. Once approved by the DITCOM approval for the purchase of the eMobilitiy devices is obtained from the Department's Chief Financial Officer and the Head of Department.

(d) After DITCOM approval has been granted, the completed VPNC request must be emailed in PDF format to pgwc-eMobility@westerncape.gov.za

(e) Once approved by the Head of Department, the order is placed with the service provider to procure the required eMobility devices.

(f) The standing instructions to the relevant data card service provider must be to supply data cards with the wild card, voice, SMS and MMS applications removed on the PGWC part of the card.

(g) On the Hybrid side, open access with a SMS option will be available. However NO VOICE function will be available. The Hybrid side will only operate as a "pay as you go" option.

4. RENEWAL/EXTENSION OF eMOBILITY CONTRACTS

(a) Renewal is permissable after a 24 months period.

(b) Renewal is not automatic but strictly depends on the usage of the device within the contract period.

(c) Usage is monitored by making use of the eMobility tool:

http://wcg.emobility.gov.za:8181/user/

(d) The eMobility information officer will send a reminder to the users before the contract expires.

(e) Renewal is subject to the same conditions as in the original application phase. The management will coordinate the process of the contract's renewal by ensuring that they monitor the usage of the eMobility and recommend the renewal when they are certain that the user has been using the device as required.

(f) The renewal application form must be fully completed and submitted prior the expiry date/s of the contract/s.

5. CONDITIONS FOR NON-RENEWAL

(a) Where the user does not use the device optimally.

(b) Failure to submit closure report from Loss Control when the user has lost the device.

(c) Incomplete application forms.

(d) Where the user has failed to submit the documentation a month before the eMobility service expiry date.

6. ISSUING OF THE eMOBILITY DEVICES

(a) On receiving the device, the user must sign an acknowledgement receipt confirming that the device was issue to she/he has been issued with the sim card and the eMobility device.

(b) The user must return the old device to the eMobility information officer before s/he can be re-issued with a new device.

(c) The same SIM card will be used in the new contract.

(d) The user is the owner of the device and it is his/her responsibility to ensure that it is kept safe.

7. DISPOSAL OF OLD MODEMS

(a) eMobility devices returned to the eMobility information officer will be disposed of in accordance with the Department's disposal policy, procedures and process.

(b) The Departmental disposal committee will provide guidance on how to dispose the modems as recommended in the disposal policy.

8. HOW MUCH CAP IS RECOMMENDED?

CAP

(a) The standard CAP size recommended is 350M.

(b) Applicants who require a CAP that is more than 350M must submit a written motivation and budget holder approved application to the DITCOM detailing why an upgrade is required.

(c) Total CAP will be calculated taking into account whether the applicant is also a recipient of cellphone reimbursement as per the transversal cell phone policy of the Western Cape Government.

(d) DITCOM will make recommendations regarding proposed data usage upgrade requested by the applicant.

(e) An eMobility change control form must be completed by the user and signed by the management requesting the upgrade of the CAP. The change control form is available on Livelink landing (home) page.

(f) Once the DITCOM has approved the request for upgrade, the eMobility information officer will forward it to SITA for implementation.

COSTS

(a) While eMobility is a new model for controlling the use of data cards, the budget holder is responsible for cost of the 24month contract.

(b) In this case it will be the monthly fixed bill for the device.

(c) Accounts are centrally paid on a monthly basis by the Department's Finance Directorate and payments are made against a programme or regional budget.

9. INTERNATIONAL ROAMING

(a) The Department does not permit international roaming unless approved via submission by the Department's Accounting Officer.

10. LOSS, THEFT AND MULTIPLE USE

The section below references the Transversal policy section 10. LOSS, THEFT, DAMAGE AND MULTIPLE USE:

(a) All lost, stolen and damaged data cards must be reported immediately to the eMobility information officer and the Department's loss control officer. The loss control process must be followed.

(b) It is the responsibility of the user to inform the eMobility information officer, should the data card be lost, stolen or damaged.

(c) eMobility information officer will thereafter ensure the blacklisting and cancellation process with the service provider, SITA and the department.

(d) The user may not apply for a replacement unless she/he has been provided with a closure report from the Loss Control unit with the recommendation that the device be replaced.

(e) Officials issued with eMobility devices must ensure that the data cards are safely kept when not in use.

(f) eMobility data cards may not be left unattended in vehicles or unlocked offices.

(g) Officials should not swap data cards without communicating the information to the eMobility information officer.

(h) In the event where the official does not require the device anymore, it must be returned to the eMobility information officer.

(i) In case of multiple users (where it seems impossible not to share a data card) the user to whom the device has been issued must keep a logbook of details that indicates who used the card on specific dates and specific times.

(j) The DITCOM must be informed of this change and must give the relevant approval (This procedure must be a last resort as this will prompt sharing of not only the device but also the cap). The above is a RICA requirement.

11. SUMMARY OF RESPONSIBILITIES

Officer	Responsibility
Official's supervisor and regional/budget manager/director	Is responsible for motivation and approval of the application and suggested data-use cap to DITCOM.
The official requesting a data device	Is responsible for supplying all relevant information as indicated on the eMobility application form. Safekeeping and proper use of the eMobility device is the responsibility of the user/official.
Department	For assigning an eMobility officer To liaise between the department and the eMobility Forum To verify the official's need for a mobile data device To verify the motivated data cap To decide on the service provider
eMobility information officer	Is responsible for executing the DITCOM request and to acquire the data devices Is responsible for sitting on the eMobility Forum's monthly meeting where all card issues will be raised and solved. Officer will give input to DITCOM and act as liaison between department, the eMobility Forum and the data card user. She or he should be able supply basic support if possible, if not, she or he may refer the user to the dedicated helpline (0800106443)
Data card service providers	Must adhere to the PGWC and department's data card policy and official SLAs. They must also be present or presented at the monthly meetings of the eMobility Forum. They must make sure that all data cards requested via DITCOMs are connected to the correct APN and, once delivered, ready for immediate set-up by the relevant official. Service providers must also supply SITA with the relevant information so that the cards can be activated on SITA servers.
SITA	Responsible for setting up SLAs with service providers on behalf of the PGWC.

Officer	Responsibility
	They must adhere to the National Data Card Policy and proxy rules as set out by the NIA and abide by the departmental proxy rules. Must also be present at the meetings of the eMobility Forum.
Ce-I (DDG)	Responsible for updating and applying the Mobile Data Policy for the PGWC (making sure that the department comply with the policy) and for making sure that all SLAs am adhered to.
	The relevant support systems, including the PGWC Service Centre and the SITA Service Centre (including dedicated support provided by SITA) must deliver quick and satisfactory service after a call has been logged.

....

Head of Department

Date 19/12/2013

ANNEXURE DSD-A

ANNEXURE

DSD-A: e-MOBILITY APPLICATION FORM

Date:	**REQUESTOR**		
Name:			
District / Directorate:			
Title / Rank:			
Delivery Location:			
Contact number:		Persal number:	
e-mail address:			
Employment Status	Permanent □ - Temporary □ *(if temp explain long-term plans for equipment)*		
Laptop Details	Model	Barcode	Serial No
Reason required	New equipment□ / Replacement equipment □		
EQUIPMENT/SERVICES REQUIRED		**Qty**	**Approx Value**
eMobile:			**R85.00 p/m**
BAS Details: Objective	Regional Identifier	Responsibility	

I am aware of and accept the terms of the Provincial IT, End User, Internet / Intranet and E-mail policies and accept responsibility for safeguarding the assets assigned to me.		
Requestor name:	**Signature**	**Date:**
This equipment / service is required to meet the user's job requirements and is the most economical option to ensure effective and efficient service delivery.*(where signatory is in an acting position, letter of authorisation to be attached, for auditing purpose)*		
User's supervisor name	**Signature**	**Date**
Director / Regional Manager name	**Signature**	**Date**

Submit to the DITCOM Secretariat: 5th floor Union House, Queen Victoria St Cape Town

*** * * SECRETARIAT USE ONLY * * ***

□	This application is complete and in line with policy and therefore recommended for approval.
□	This application is incomplete and is returned to the applicant.

Secretariat name:	**Signature:**	**Date:**

Approval	
□	This application is in line with policy and approved
□	This application is rejected by the IT Management Committee for the following reasons:

Chairman name	**Signature**	**Date**

ANNEXURE DSD-B

DSD-B: DATA CARD APPLICATION

Departmental Service Provider: MTN

ID Number:				
Name and Surname:		**Rank:**		
Branch/Directorate:		**Location:**		
Contact Number:		**Persal No.:**		
Data Card Sim No.:		**MSISDN**		
Huawei modem		**Huawei S/NO**		
Physical Address:				
CAP required/approved	350M □	500M □	700M □	1Gig □

Declaration

- I undertake to limit the usage of the data card for effective service delivery. I understand that the data card can be withdrawn due to misuse.
- I will take the necessary precautions to protect the data card against theft, loss, breakage and unauthorised use. I undertake to immediately report the loss of or damage to the data card to the relevant Supply Chain Management unit, Loss Control Officer and e-Mobility Officer.
- **I acknowledge that log files, traces and intercepts of any traffic passed via this service may be made, utilised and stored in terms of the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002) and, by my signature hereto, do give assent to all such actions without reserve.**
- Should I fail to comply with the above, and the provisions of the Data Card Policy, this certification will serve as a mechanism to withdraw the data card and take action against me according to relevant legislation.

User name	**Signature**	**Date**

	The user represents one or more strategic functions within the Department
	This user regularly performs tasks of a critical or urgent nature and needs to use e-mail or other internet systems whilst away from the office or after hours.

	This user needs to use e-mail or other internet based systems and cannot get access to these systems through other cheaper or more effective communication methods

Recommendation by Sub-Programme Manager

Other Comments:

Supervisor's name	**Signature**	**Date**

APPROVED/NOT APPROVED

Funds are available in the user's Cost Centre Budget to apply for eMobility

Manager(Director)/Regional Manager's name (Budget Holder)	**Signature**	**Date**

DSD-B: e-MOBILITY APPLICATION CHANGE CONTROL FORM

Date:	
Department	
District / Directorate:	
Title / Rank:	

Username		Persal number	

Device MSISDN (SIM) Number:	

Current CAP										
Requested new CAP	**350M**		**500M**		**700M**		**1GIG**		**2GIG**	

Motivation for request

Declaration

- I undertake to limit the usage of the data card for effective service delivery. I understand that the data card can be withdrawn due to misuse.
- I will take the necessary precautions to protect the data card against theft, loss, breakage and unauthorised use. I undertake to immediately report the loss of or damage to the data card to the relevant Supply Chain Management unit, Loss Control Officer and e-Mobility Officer.
- **I acknowledge that log files, traces and intercepts of any traffic passed via this service may be made, utilised and stored in terms of the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002) and, by my signature hereto, do give assent to all such actions without reserve.**
- Should I fail to comply with the above, and the provisions of the Data Card Policy, this certification will serve as a mechanism to withdraw the data card and take action against me according to relevant legislation.

Requestor name:	**Signature**	**Date:**

This service is required to meet the user's job requirements and is the most economical option to ensure effective and efficient service delivery. Funds are available in the user's Cost Centre Budget to apply for eMobility upgrade ***(where signatory is in an acting position, letter of authorisation to be attached, for auditing purpose)***

User's supervisor name	**Signature**	**Date**
Director / Regional/Budget Manager (Name)	**Signature**	**Date**

Submit to the eMobility Officer: 2nd floor Union House, Queen Victoria St Cape Town

*** * * SECRETARIAT USE ONLY * * ***

□ This application is complete and in line with policy and therefore recommended for approval.		
□ This application is incomplete and is returned to the applicant.		
DITCOM Secretary name:	**Signature:**	**Date:**

Approval		
□ This application is in line with policy and approved		
□ This application is rejected by the IT Management Committee for the following reasons:		
DITCOM Chairman name	**Signature**	**Date**
SITA received		

Annexure DSD-C

DSD-C: Glossary of Terms

APN	Access Point Name means cellular technology based on Global System for Mobile Communication and refers to a secure point of entry into a network.
DITCOM	The Departmental Information Technology Committee
WCG	Western Cape Government
Officer/Officials	all persons in the employment of the WCG
SITA	State Information Technology Agency
RICA	Regulation of Interception of Communications and Provision of Communication –related Information Act, 2002 (Act 70of 2002)
SLA	Service –level Agreement
VPN	Virtual Private Network (usually where departmental applications reside).
VPNC	Virtual Private Network Client (giving an official access to the VPN where departmental applications are hosted)
MSISDN	The cell number of a data card provided in international format.
eMobility officer	The Information and Communication Technology manager at Knowledge Management.

Appendix A

WCG Transversal

Data Card Policy: eMobility

Approved Version 2.40

20 August 2012

Western Cape Government

Department of the Premier

Branch: Centre for e-Innovation
E-mail: Lance.Williams@westerncape.gov.za
Tel: +27 21 483 5565 Fax: +27 21483 5539

Enquiries: Lance Williams

Data Card Policy: eMobility
Approved Version 2.40
20 August 2012

1. BACKGROUND

The authority to adopt a transversal WCG policy on the use of cellular data cards for official purposes is vested in the Western Cape Government (WCG).

The data card permits a secure link to applications on the WCG network from any place with cellular data reception where cheaper and more effective communication methods do not exist.

Since a user connected by an eMobility data card logs on to the Access Point Name (APN) and the WCG network, access to applications (including the Internet) will be managed in terms of the normal existing policies.

This eMobility data card policy is a transversal policy and replaces previous and existing data card policies for all departments of the WCG.

The current problems with data cards, such as unsecured network access, high costs to departments and lack of governance of the existing departmental policies, necessitate a new paradigm, called eMobility.

2. AIM

The aim of this document is to regulate and standardise the practices and procedures for the acquisition, provisioning and use of data cards in the WCG and its departments in order to enable the Director-General, as well as all departmental accounting officers, to manage this essential service in a cost-effective and well-governed manner.

3. PRINCIPLES

This policy is based on the following principles:

- A data card is a work facility and the allocation thereof does not constitute a fringe benefit and therefore should be used for official purposes only.
- As a work facility, it remains the property and responsibility of the Western Cape Government and therefore departments must ensure that data devices are properly accounted for in terms of financial guidelines (PFMA).
- The WCG, through its departments, is responsible for managing the physical and financial risks related to the use of data cards.
- This policy takes the PFMA, RICA as well as the current WCG Internet Policy into account.
- All WCG hardware and software standards are adhered to – take note that the WCG has standardised on the Microsoft platform. No other platform/s will be supported until further notice. In the case of PADS & TABS as well as other Smart Devices not on the Standard Equipment list the WCG (Ce-I) will only support eMobility when these devices are utilized to connect to WCG systems via 3G and not the devices or application running on these devices. All these devices must be able to run VPNC (IP Sec.) as embedded software as well as having the capability to switch between at least two profiles to enforce proxy settings.

4. DEFINITIONS AND EXPLANATIONS

For the purposes of this document:

- APN (Access Point Name) means cellular technology based on Global System for Mobile Communications (GSM) and refers to a secure point of entry into a network.
- DITCOM means Departmental Information Technology Committee. (Naming may vary from department to department including RITCOM, BITCOM etc. but the function basically stays the same.)
- DPSA means Department of Public Service Administration.
- NIA means National Intelligence Agency.
- Officers/officials mean all persons in the employment of the WCG.
- PFMA means the Public Finance Management Act, 1999 (Act 1 of 1999).
- WCG means the Western Cape Government.
- RICA means Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002).
- SITA means the State Information Technology Agency.
- SLA means Service-level Agreement.
- VPN means Virtual Private Network (usually where departmental applications reside).

- VPNC means Virtual Private Network Client (giving an official access to the VPN where departmental applications are hosted).
- Wild card means the application that provides the data card with the ability to allow the user open and free access to all Internet sites with no governance and no restrictive access to certain websites.
- MSISDN number is the "cell" number of a data card provided in international format.
- SM means services manager.
- TM means technology manager.
- Hybrid means the dual nature of the sim: eMobility profile with full governance and the Service Provider profile to include a "pay as you go" option for normal use where the expense is **not** for the account of the WCG.

5. SOME BENEFITS OF THE eMobility (Hybrid) SYSTEM

a) The latest eMobility system (called eMobility Hybrid) is a world first and unique to the WCG.

b) The Hybrid card has a dual integrated nature, allowing full governance on the WCG side and open access on the Service Provider side. The open access part of the sim must be seen as "pay as you go", This is an option and when used the cost will be for the user's own pocket. This has no implication for the WCG and holds no threat or cost towards the WCG.

c) Each month a predetermined amount of data will be allocated to each sim provisioned to the Hybrid system. This comes at no extra cost to the WCG and is deemed to allow connectivity should any of the eMobility systems fail.

d) When the "hybrid" data has been depleted during any given month, the Hybrid part will stop functioning until topped up like any other normal 3G "pay as you go" data card.

e) Governance is in place and can be monitored on the WCG part of the card.

f) Wild card access, voice, SMS and MMS applications have been removed from the official WCG part of the card.

g) Fixed costs for provincial departments:

   i) no SIM association fees (a fee payable whether the card is used or not)

   ii) no SITA costs to the user / department.

h) Large departments (+200 data card users) can have their own sub-APN which will allow governance.

i) Data caps can be allocated to users by departments and monitored.

j) APNs are now local (situated in the Western Cape) and this should enhance data speed as it eliminates back-hauling of data traffic.

6. PROCEDURE FOR ACQUISITION AS OPERATIONAL LEASE, INCLUDING VPNC (ALSO SEE ANNEXURE B)

Application and motivation must be submitted to the relevant DITCOM (departmental IT committee) of each department. Once DITCOM approval has been granted, the approval is then forwarded to the supply-chain management unit of each department that facilitates the LOGIS and procurement process further. The standing instructions to relevant data card service providers must be to supply data cards with the wild card, voice, SMS and MMS applications removed on the WCG part of the card. On the Hybrid side open access with a SMS, MMS as well as voice functions will be available. The Hybrid side will only operate as a "pay as you go" option to make provision for the latest web enabled Smart Phones.

The DITCOMs must assure themselves that the applicant needs a data card for official purposes and that the application is motivated by the official's senior manager who also indicates the needed data cap for the particular official. DITCOMs must ensure that the RICA information is captured. Furthermore, the applicant must include the prescribed completed *VPNC* form should she or he like to have access to applications that are not web-enabled or located behind the firewall in the VPN. After DITCOM approval has been granted, the completed *VPNC* request must be e-mailed in PDF format to pgwc-emobility@sita.co.za.

7. eMOBILITY OFFICERS

Each department must assign an official, preferable not lower than post level 9, to be responsible for the issuing of data cards on behalf of that department. This official will also represent that department on the eMobility Forum. This forum will meet monthly to discuss data card issues. SITA and data card service providers will also attend this forum. It will be expected of the eMobility officer to give feedback to the relevant DITCOM and department. Basic training will be provided to eMobility officers to assist them with basic support. (See Intranet "Applications" for updated eMobility Officers list.)

8. APPLICATION FOR ACCESS TO THE eMobility APN AND VPNC

a) Once the card is procured via the DITCOM process, it will be activated on the eMobility APN. The official receiving the card will have to do a card set-up. Guidelines for the set-up of cards can be provided and is published and updated on the WCG Intranet. eMobility officers should also be able to assist.

b) The official in need of access to applications residing in the VPN (e.g. the Hospital Information System or EduInfoSearch which are protected by the VPN firewall) must complete the VPNC request form. (The form can be downloaded from https://vpnc.gov.za or is obtainable in hard copy from the eMobility officers. See ANNEXURE B.) This request goes through the DITCOM approval process. Should the official only need to access the Internet and web-based applications, the VPNC request will not apply.

c) The official will have to run and set up VPNC on his or her computer. Information will be provided via an e-mail sent from SITA. The eMobility officer, SM or TM should be able to assist with the set-up.

d) Within 24 hours after receiving the data card, the eMobility system should be operational (provided that the official has completed the set-up correctly).

e) Should the official have difficulty in setting up the card or should he or she experience problems with the VPNC set-up, he or she must log a call with the eMobility-VPNC dedicated helpline (0800106443) from where it will then be escalated. When logging a call, the official should state immediately whether the problem relates to eMobility, VPNC or to both.

f) Ultimately VPNC requests, both Group Policies and User Applications, should be signed by the "Owners" of these policies – on a level not lower than a director. Each department should have "owners" for these policies to regulate and monitor users on the WCG back bone. Completed VPNC Group Policies as well as User Applications must be e-mailed in PDF format to pgwc-emobility@sita.co.za

9. PROCUREMENT OF DATA CARDS – OPERATIONAL LEASE: SERVICE PROVIDERS

Procurement of data cards may only be done via MTN and or Vodacom. Cellular footprint (coverage), pricing and service-provider service will determine the choice of network provider. The contract cost for data cards *will be an obligation between the department and the service provider*. Departments, therefore, should follow their departmental supply-chain management process to procure new or additional data cards while keeping the prescripts of this policy in mind. It is important to clearly state "eMobility Hybrid" in the application.

10. LOSS, THEFT, DAMAGE AND MULTIPLE USE

All lost, stolen or damaged data cards must be reported immediately in terms of the financial prescripts to the eMobility officer of that department as well as to the loss-control officer of that department.

Officials must ensure that data devices are always kept secure when not in use and officials will be held liable for the replacement of such a device in the event of it being lost, stolen or damaged due to his or her failure to keep the device in a secure place. Data-card devices may, for example, not be left unattended in vehicles or in unlocked offices, etc.

It is the responsibility of the user to also notify the departmental eMobility officer *immediately* should the data card be lost, stolen or damaged. The eMobility officer will facilitate the process further with the service provider, SITA and the department. Each data-card user must activate a security PIN number (refer to documentation issued with data card) for security reasons. The security PIN number and data device may *not* be shared or made available for use by anybody other than the official to whom it was issued.

In *extraordinary* situations where it seems *impossible not to share* a data card, the department responsible for that card *must* have a logbook of detailed use drawn up via their eMobility officer or DITCOM to indicate who used the card on specific dates and at specific times. The DITCOM of such a department must be informed of this change and must give the relevant approval. (This procedure must be a last resort as this will prompt sharing of not only the device but also the cap of the device as well as the safety PIN number.) The above is a RICA requirement.

Take note: this concession *only applies* to a single device with a unique IP address per user and *not* to a device with a single IP address to multiple users. This type of usage nullifies governance.

11. UPGRADING OF DATA-CARD CONTRACTS

When the contract of an official using a data card comes up for renewal, the eMobility officer will inform the departmental DITCOM. It is the responsibility of the official's supervisor to motivate in writing that the current user of the data card is still entitled to such a device and this will go through the review process via the relevant departmental DITCOM (refer par. 6). The replaced equipment (data device) must be dealt with in terms of financial guidelines (PFMA and Treasury guidelines). The SIM of the device stays in use and must be placed in the new (upgraded) device. DITCOMs or departments must take financial prescripts (PFMA) into account when disposing of replaced devices.

12. MONITORING AND EVALUATION

Monitoring of WCG data cards will be facilitated by the eMobility officers who will submit monthly reports to the relevant DITCOM. The Western Cape Government reserves the right to withdraw data service from officials in cases where misuse is reported by eMobility officers. Departmental DITCOMs will make recommendations regarding changes to officials' data-usage caps via a change control process in collaboration with eMobility officers. Standard cap levels are set by default at 350 MB per user if not specified otherwise. (See ANNEXURE D.)

13. IMPLEMENTATION

This policy is applicable to all officials and departments of the WCG; this includes permanent employees, employees that have been employed on contract or on a temporary basis as well as seconded staff. This policy serves as a transversal umbrella policy regarding data cards. Where a particular department is not in a position to implement the data card policy with immediate effect, such a department must supply valid reasons in writing to the DDG (Ce-I) and indicate time frames for its implementation. In such cases this policy must be phased in as soon as possible.

14. COSTS

While eMobility is a new model for controlling the use of data cards, *departments will only be responsible for paying contracts concluded between themselves and service providers*. In this case it will be the monthly fixed bill for the device. Payment for *data usage*, APNs, etc. will be for the account of the WCG until further notice. (Calculations generally indicate a saving by departments of up to 70%.)

International roaming ***will be for the cost of a department***. This is a potentially very expensive option and is to be discouraged. Best practice has shown that it is best to buy a pre-paid sim bundle from the country that is visited. Normal roaming can not be guaranteed. Special permission to request international roaming services must be obtained via the DITCOM of a department, supplying full details of the period this service will be required. This action will take place between a department and a service provider and falls outside the scope of eMobility as roaming is disabled on the eMobility sim.

15. ASSISTANCE, HELP AND SERVICE CENTRE (SEE ALSO ANNEXURE C)

When assistance or help is needed regarding eMobility and/or VPNC, the first step would be to contact the eMobility officer of the specific department. If the eMobility officer is unable to help, it can be of great value to include the SM or TM in this process.

Should the need to log a call for assistance still arise, the official must make use of the **0800106443** number provided on ANNEXURE E. (See diagram for explanation.) Take note: the person logging the call must be able to provide basic personal information, ***including*** the MSISDN number of the device in international format (Example: 27729330420). This number must be supplied to the user by the department that issued the device via the eMobility officer.
It is also important to mention to the operator who takes the call that the person logging the call is from the WCG and requires a call to be logged under "eMobility/VPNC Western Cape".

All the latest eMobility tips, tricks, tools, information and setup guides are regularly published on the WCG Intranet. (http://intrawp.pgwc.gov.za – see "Applications")

16. SUMMARY OF Rolls and RESPONSIBILITIES

The official's manager is responsible for motivating the application and suggested data-use cap to DITCOM.

The official requesting a data device is responsible for supplying all relevant information as indicated on ANNEXURE A and he or she is responsible for the device as well as the SIM in the device.

DITCOMs or departments are responsible for assigning an eMobility officer to liaise between the DITCOM or department and the eMobility Forum, to verify the official's need for a mobile data device, to verify the motivated data cap, to decide on the service provider and to notify the supply-chain unit.

Each department's supply-chain unit is responsible for executing the DITCOM request and to acquire the data device. The department's eMobility officer is responsible for sitting on the eMobility Forum's monthly meeting where all data-card issues will be raised and solved. This officer will also give input to DITCOM and act as liaison between DITCOM, the eMobility Forum and the data card user. He or she should also be able to supply basic support if possible; if not, he or she may refer the user to the dedicated helpline (0800106443).

Data card service providers must adhere to the WCG data card policy and official SLAs. Service providers must also be present or represented at the monthly meetings of the eMobility Forum. They must make sure that all data cards requested via DITCOMs are connected to the correct APN and, once delivered, ready for immediate set-up by the relevant official. Service providers must also supply SITA with the relevant information so that the cards can be activated on SITA's servers.

SITA is responsible for setting up SLAs with service providers on behalf of the WCG. They must adhere to the National Data Card Policy and proxy rules as set out by the NIA and the DPSA. SITA must also adhere to the SLA between the WCG and SITA and abide by departmental proxy rules. SITA must also be present at the meetings of the eMobility Forum.

The Ce-I (DDG) is responsible for updating and applying the Mobile Data Policy for the WCG (making sure that departments comply with the policy) and for making sure that all SLAs are adhered to.

The relevant support systems, including the WCG Service Centre and the SITA Service Centre (including the dedicated support provided by SITA), must deliver quick and satisfactory service after a call has been logged.

Lastly, *all* partners and stakeholders mentioned in this policy should work together as one team to deliver a seamless, robust, reliable and cost-effective service that will add value to the WCG (applying the PSO 12 objective to be the Best Run Provincial Government in the World) and ultimately improve the lives of the citizens of this province.

03/12/2012

Mr LR Williams
DDG: CENTRE FOR E-INNOVATION

Date

03/12/2012

Mr A Joemat
SUPERINTENDENT-GENERAL: CORPORATE SERVICES

Date

4/12/2012

Adv B Gerber

DIRECTOR-GENERAL : WESTERN CAPE GOVERNMENT

Date

ANNEXURE A

Example: Data card application form (to be included in DITCOM application)

ID no.:

Name: **Rank:**
Branch/Directorate: **Location:**
Contact number: **Persal no.:**
Data-card SIM no. (as soon as available):
Physical address:

CAP required/approved: 350 MB / 500 MB / 700 MB / 1 GB / 2+G

Declaration

I undertake to limit the use of the data card for effective service delivery. I understand that the data card can be withdrawn due to misuse.

I will take the necessary precautions to protect the data card against theft, loss, breakage and unauthorised use. I undertake to report the loss of or damage to the data card immediately to the relevant supply-chain management unit, loss-control officer and eMobility officer.

I acknowledge that log files, traces and intercepts of any traffic passed via this service may be made, used and stored in terms of the provisions of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002), and I, with my signature hereto, assent to all such actions without reserve.

Should I fail to comply with the stipulations above and the provisions of the Data Card Policy, this certification will serve as a mechanism to withdraw the data card and take action against me according to the relevant legislation.

User name **Signature** **Date**

Recommendation by sub-programme manager:

	The user performs one or more strategic functions in the Department.
	This user regularly performs tasks of a critical or urgent nature and needs to use e-mail or other Internet systems while away from the office or after hours.
	This user needs to use e-mail or other Internet-based systems and cannot get access to these systems through other cheaper or more effective communication methods.

Other comments:

Name of supervisor name **Signature** **Date**

APPROVED / NOT APPROVED

Sub-programme manager **Signature** **Date**

ANNEXURE B

VPNC Services Application

PO BOX 26100; MONUMENT PARK;

A. DETAILS OF APPLICANT (Full details)	FOR SITA USE ONLY
***Full Name & Surname:**	**ARS Reference no:**
***Department:**	****Acc Manager name:**
VPN to be accessed:	
***E-Mail address:**	****Signature:**
***Telephone no:**	****Date:**
***Fax no:**	****SITA WA no:**
Application Type: New / Update / Delete	**Departmental code:**

B. THE SERVICE IS SUBJECT TO THE FOLLOWING TERMS and CONDITIONS:

1. **Mandatory fields for User are indicated with * and for Account Manager **.**
2. **This application must reach SITA Converged Communications via your Account Manager from 1 April 2009. If you require any assistance completing this application form, please contact your SITA Account Manager or Business Portfolio Consultant.**
3. **No service will be handled as URGENT unless a written motivation is attached to this form.**
4. **Departments are responsible for the supply of any required bearer network used to enable connectivity to the VPNC service.**
5. **SITA will make the VPNC client software available online for all major operating systems.**
6. **This application form needs to be approved by all the relevant Group Policy owners.**
7. **Access accounts that remain inactive for a period of 30 calendar days or more will be suspended and may be revoked or cancelled without further notice to the** user **after 90 days.**
8. **You will be provided with a reference number which is required for all enquiries.**
9. **The security undertaking is compulsory. Incomplete or incorrect completion of this section will result in the summary rejection of the application.**
10. INDEMNITY: ***SITA will not be held responsible for fraudulent use of scanned signatures on this request form.***

C: SECURITY UNTERTAKING: User

***I, the undersigned, _______ ____________________________ hereby undertake that the provisions of any and all security/group policies applicable to the VPN or resources to be accessed, as amended from time to time, shall be fully complied with in respect of the services applied for in this document.**

Specifically, without dilution or modification of the intent or definition of anything stated within such policies:

1. **I undertake to ensure that the services provided by SITA shall only be used by duly authorized persons for official purposes.**
2. **The access credentials issued to an individual are to be kept secret and known only to that individual concerned. I accept that such access credentials are my personal responsibility and that I shall be held accountable for any and all actions or utilization associated with such access credentials. I further stipulate that authentication server records shall constitute proof of such use.**
3. **I acknowledge and accept that log files, traces, intercepts and other monitoring of traffic carried via this**

service may be made, utilized and stored in terms of the provisions of the RIC Act (Act 70 of 2002) and do hereby give my fully informed consent to all such actions.

4. Physical and/or electronic audits of any/all equipment connected to the SITA network may be performed at any time with or without prior notification.
5. Discovered or learned violations of any aspect of the GOV security policy SECPOL2001 or applicable VPN security policy may result in partial or complete suspension of services provided by SITA with or without prior notification.

***Signed at ______ _____________ on this day _______ of _____ ___________ 2010___.**

***Signature: ____**

D. Security Undertaking: Group Policy Owner

*** I, the undersigned** Group Policy Owner, **do hereby warrant that I am a duly authorized representative of the department indicated on page one.**

I further warrant that the undertaking made here shall be held to be binding on the abovementioned department and that I am authorized to make such an undertaking.

Therefore, I undertake that the provisions of any and all security/group policies applicable to the VPN or resources to be accessed, as amended from time to time, shall be fully complied with in respect of the services applied for in this document.

.

Specifically, without dilution or modification of the intent or definition of anything stated within the GOV security policy SECPOL2001 or applicable VPN security policy:

1. **Services provided by SITA shall only be used by duly authorized persons for official purposes.**
2. **Undertake to inform all users of this service that all their access credentials issued to an individual shall be kept secret and known only to that individual concerned.**
3. **Physical and/or electronic audits of any/all equipment connected to the SITA network may be performed at any time with or without prior notification.**
4. **Discovered or learned violations of any aspect of the GOV security policy SECPOL2001 or applicable VPN security policy may result in partial or complete suspension of services provided by SITA with or without prior notification.**

POLICY GROUP	POLICY GROUP REFERENCE NUMBER	POLICY GROUP OWNER	SIGNATURE

Comments: (in block letters)

ANNEXURE C

PROCESS FLOW:

1 **A need arises for the use of a data card:**

The official completes the DITCOM application as well as ANNEXURE A – SMS member approves application – DITCOM approves and notifies the department's procurement system.

Procurement acts on DITCOM recommendations and procures card from a service provider (MTN/Vodacom).

The service provider aligns the SIM of the device to the WCG's APN and passes the relevant information on to SITA – SITA sets up the user information on the Radius server.

Device is delivered to official – eMobility profile is set up by official – eMobility immediately provides governed access to all web-based applications and open access on the Hybrid side (cost for users pocket- "pay as you go").

Should VPNC be required:

Applicant completes VPNC User Application (ANNEXURE B) – DITCOM approves and "owner" of the policy signs document.
Completed form is e-mailed in PDF format to pgwc-emobility@sita.co.za.
SITA responds by sending set-up procedures to the applicant by e-mail.
Applicant/user/official sets up VPNC.

2 **Assistance/help is needed:**

Get hold of the eMobility officer for basic support.
If the problem cannot be solved, get the SM/TM involved.
Should a call be logged, call 0800106443 (See ANNEXURE E).

3 **Data cap to be changed**:

Complete ANNEXURE D – SMS member recommends – DITCOM approves.

Completed form handed to the eMobility officer. eMobility officer relates this information to the local dedicated eMobility-VPNC support staff in PDF format via pgwc-emobility@sita.co.za. All copies of request forms must be filed.

Western Cape
Government

Department of the Premier

ANNEXURE D

Change Control Form: *Changing the cap for an eMobility user*

Date: ____

Department: ____

User name: ____

Device MSISDN (SIM) number: ______________________________

Current cap: ____

Requested new cap: ______________________________________

Motivation for request: ___________________________________

____

____

____

____

Signature of user: ____

Signature of SMS member (approving manager): _______________

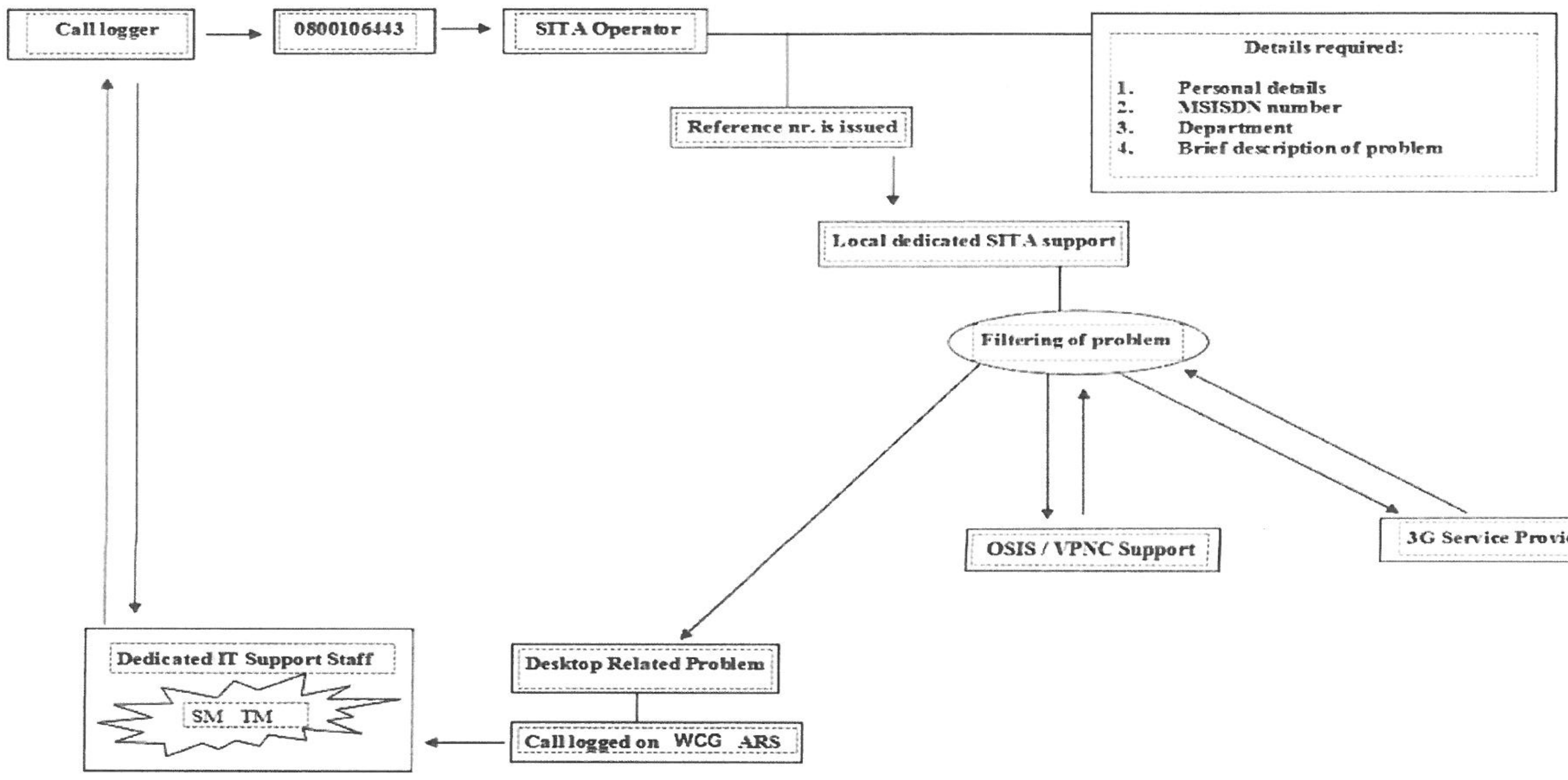
____

DITCOM approved: ____
(Signature and date)

SITA received: ____
(Signature and date)

ANNEXURE E

Procedure for logging eMobility / VPNC calls: Must state to operator: " WCG official, logging a call under eMobility / VPNC Western Cape"



MR. J. O. SMITH
CHIEF FINANCIAL OFFICER

Telephone: 021 483 8678
Facsimile: 021 483 8607
E-mail: Juan.Smith@westerncape.gov.za

MEMO

[✓ [ ] URGENT] [ ] FOR COMMENT [ ] PLEASE REPLY [ ] FILE

TO: Denver Holley / Nigel Arendse

Ple peruse policy with specific reference to para 8 - "costs" and para 10 "losses"

Regards

JSmith
29/11/2013.

Par 10 :- Is fine, as it is inline with current draft Policy.

Par 08 :- Concern wrt to Finance lease: Noel :-

① Recommend that this service be linked to existing cellphone contracts to minimise cost. ② Also to note that existing cellphone contracts (most) comes with free data.

③ Furthermore, the role out of this service to lower levels contradict the actions taken wrt cell phones (outsourcing) as it can be seen as a means of replacement.

④ Access to e-mails do exist at all Regional + Local offices

⑤ This service be restricted to essential services only

- SMS
- Service pack off-site

2013/3937

Western Cape Government

Social Development

Allison.Thomas@pgwc.gov.za
Directorate: Research, Population and KM
Tel: +27 21 483 4355: Fax: +27 21 483 3912
14 Queen Victoria Street, Cape Town, 8001

6/4/3P

REFERENCE :
ENQUIRIES: Allison Thomas

ROUTE FORM:

SUBJECT: EMOBILITY POLICY

Name	**Signature**	**Date**
Gavin Miller Director: Research & Knowledge Management		2013-11-27
Marion Johnson Chief Director: Business Planning & Strategy		27/11/13
Charles Jordan **Chief Director: Social Welfare**		27/11/13
Mzwandile Hewu Chief Director: Community & Partnership Development		2013/11/29
Juan Smith Chief Financial Officer		12/12/2013
Robert Macdonald Head of Department		19/12