OFFICE OF THE PREMIER ACCESS CONTROL POLICY

THE ACCESS CONTROL POLICY

1. Purpose

1.1 To propose for the introduction of an ID card policy for the Office of the Premier.

2. Background

2.1 The Office of the Premier has installed the technical access control system at the 26 Bodenstein Offices. For the system to function effectively proximity cards should be issued to members for use.

2.2 The identity cards are regarded as work facilities as well as security tools and are made available to users primarily to enable them access to the Office of the Premier premises. Every employee of the Office the Premier is issued with the proximity card. The cards are supplied by the Security and Risk Management Strategies.

2.3 The ID cards need to be properly controlled as they can enable the user access to premises, which may compromise classified information and assets.

Proposed new policy

3. Introduction

3.1 The issue and strict control of identity cards is crucial to ensure a safe and secure working environment. Office of the Premier identity cards is an integral part of any physical and technical access control system or procedure. Other than just being a means to positively identify employees, government

Identity cards can be used to track movements of the cardholder on sites where technical security systems are installed. Security and Risk Management Strategies is responsible for the manufacture, issue and control of the Premier's Office identity cards. Individual identity card holders are responsible and accountable for their cards and how and where they are used. Where external contractors are issued with the Premier's Office contractor identity cards, the line management by whom they are appointed, is responsible for control, use and return of the cards.

4. CONTROL OF ACCESS TO PUBLIC PREMISES AND VEHICLES ACT 53 OF 1985 AS AMENDED.

(1) Notwithstanding any rights or obligations to the contrary and irrespective of how those rights or obligations arose or were granted or imposed, the owner of any public premises or any public vehicle may-

(a) Take such steps, as he may consider necessary for the safeguarding of those premises or that vehicle and the contents thereof, as well as for the protection of the people therein or thereon.

(b) Direct that those premises or that vehicle may only be entered or entered upon in accordance with the provision of subsection (2).

(2) No person shall without the permission of an authorized officer enter upon any public premises or any public vehicle in respect of which a direction has been issued under subsection (1) (b), and for the purpose of granting of that permission an authorized officer may require of the person concerned that he/she-

(a) Furnish his/she name, address and any other relevant information required by the authorized officer.

(b) Produce proof of his/her identity to the satisfaction of the authorized officer.

(c) Declare whether he/she has any dangerous object in his/her possession or custody or under his control.

(d) Declare what the contents are of any vehicle, suitcase, attaché case, bag, handbag, folder, envelope, parcel or container of any nature, which he has in his possession or custody or under his/her control, and show those contents to him.

(e) Subject him/her and anything, which he/she has in his possession or custody or under his control to an examination by an electronic or other apparatus in order to determine the presence of any dangerous object.

(f) Hand to an authorized officer anything, which he/she has in his position or custody or under his control for examination or custody until he/she leaves the premises or vehicle.

5. Objective

5.1 The objectives of the access control policy are to ensure that strict control guidelines over the issue, use, return and disposal of the Premier's Office identity cards and keys are provided. These controls, in conjunction with the Provincial Government Security policies and procedures will enhance the safeguarding and securing of Government's assets and employees thereby reducing the risks and threats to the Government. This in turn will assist in minimizing losses resulting from theft and unauthorized access.

6. Application for Identity Cards

6.1 Identity Cards shall only be issued on the strength of an application form that has been signed by both the applicant and his/her manager.

6.2 Application forms for Identity Cards can be obtained from the Security and Risk Management Strategies Unit.

6.3 Application forms shall be submitted at least twenty four hours prior to the issue of cards

7. Recovery of Cards

7.1 Human Resources Officer shall recover all cards from personnel whose employment has been terminated.

7.2 Human Resources shall notify Security and Risk Management Strategies in writing, on a monthly basis of the names and details of any person who left the Office of the Premier during the preceding month. On receiving such notification the Security and Risk Management Strategies will amend its records accordingly.

8. Lost /Stolen and Re-issued cards

8.1 When a card is lost, the cardholder must report the loss to the South African Police Services and the Security and Risk Management Strategies within twenty- four hours of loss.

8.2 When a card is lost, the employee must pay an amount of R50.00 for replacement of a card. The money shall be paid to revenue office. Revenue office will issue a receipt, which will be produced to the Security and Risk Management Strategies for the replacement of the card. When a cardholder is lost R20.00 shall be paid for replacement.

8.3 Where a card is damaged and needs to be replaced the damaged card must be returned to Security and Risk management strategies before a new card will be issued. A new application form will be completed for the new ID card

9. Proximity cards

9.1 Proximity cards will be issued to all personnel of the Office of the Premier who function in buildings that are fitted with electronic access control systems, or to personnel who regularly visit premises that are fitted with electronic access control systems.

9.2 Once the employee's photograph and details have been printed onto the access card, the relevant information will be captured into the access control system by the Security and Risk management strategies.

9.3 ID cards shall be worn at all times whilst on the Office of the Premier premises. ID cards shall be worn in such a manner as to be clearly visible.

10. VISITORS

10.1 Categories of Visitors

10.1.1 VIPs,i.e. Mec`s, Ministers, Director General, State President etc.

10.1.2 Official visitors i.e. for the purpose of meetings, work related matters and etc, ad hoc contractors, technicians and etc, with the exception of those mentioned in paragraph 10.1.3 below.

10.1.3 Consultants and contractors, private companies which are/were contracted on a permanent basis e.g. IBM.

10.1.4 Non-official visitors, family members, friends, relatives and etc.

10.2 Access procedures

10.2.1 **VIPs**: Protocol and Intergovernmental services will arrange for the reception and departure of the VIPs.

Security instructions shall be observed in respect to VIP visits. Any assistant required by the VIPs shall be provided with a visitor card for record purposes. The VIP has to be made aware

that such assistant has to accompany him/her constantly and also leave the building with him/her.

10.2.2 **Official Visitors**: This category must report to the access control point, go through all applicable access control procedures, and be escorted to the venue of the meeting, workplace, etc. For this purpose the host is responsible to meet the visitor at the access control point and ensure that the visitor is escorted for the full duration of his/her presence.

10.2.3 **Permanent Consultants/Contractors**: This category of vetted visitors will be issued with permanent contractor's cards, which may be coupled with access cards programmed to provide restricted access privileges only, and will be used during the contracted period only. Escorting is not essential, although the areas, to which they may not have access, must be clearly indicated to them.

10.2.4 **Family members**, friends or non-members: Such persons should be admitted to the access control point for authorization. No authority to access the premises will be provided for them without sound motivation or a justifiable reason.

10.2.5 Children up to thirteen years of age may be allowed into offices only in exceptional cases, eg when an employee takes a child to the doctor and has taken him/her back home or to the school/crèche afterwards. In such cases the Supervisor must give him/her a written approval for gaining access at the access control point. The duration of such a stay should not exceed two hours.

11. General

11.1 An official who will access and exit the premises with a visitor without authorisation by the security officials will be charged for security breach. No person shall without the permission of an authorised/security officer enter or enter upon any public premises

11.2 or any public vehicle as stated on the Control of Access to Public Premises and Vehicles Act 53 of 1985.

11.3 Without prejudice to the provisions of the Tresspass Act, 1959 (Act 6 of 1959), an authorised officer may at any time remove any person from any public premises or public vehicle if –

- That person enters or enters upon the premises or vehicles concerned without the permission contemplated in paragraph 11 above.

- The authorised officer considers it necessary for the safeguarding of the premises or vehicle concerned or the contents thereof or for the protection of the people therein or thereon.

12. OFFICE SECURITY

12.1 Each member is responsible to inspect his/her own office or work area for signs of intrusion at the beginning of each working day. If the member detects any sign of intrusion, he/she should notify the immediate head or next senior member so that the matter can be reported to Security & Risk Management Strategies immediately.

12.2 Cleaning of offices should be done during official working hours, supervised by the occupant of the office. The occupants themselves should clean offices containing sensitive apparatus or documents, which cannot be hidden/locked away.

12.3. The occupant of an office should lock the doors of the office or working area when leaving.

12.4 At the end of the day, before departure, each member should ascertain that:

- Lights and electrical appliances are switched off.
- No cigarettes, tobacco and/or matches are left burning.
- Blinds, curtains are drawn.
- Doors/windows and cabinets are closed/locked.

12.5 A register for after-hours visits to the Office has to be kept and checked monthly by the Physical and Assets Protection Manager.

13. KEY CONTROL

13.1 Security & Risk Management Strategies is responsible for key control and record keeping of keys of all offices, safes and vaults, as well as of combination codes of safes/vaults. Key control (office and cabinet keys) at regional offices is under control of the Head of the office.

13.2 Any loss of keys has to be reported immediately in writing to the Supervisor after which the security component must be informed. This case together with and affidavit must also be reported to Security & Risk Management Strategies by the person who lost the keys.

13.3 **Duplicate Keys of Head Office.** Excluding certain duplicate keys kept for emergency use, all other duplicate keys must be kept at a central point, which is under control of, and manned by the Physical Security Officer. Keys must be sealed and stored in prescribed cabinets. Only Management of the Security & Risk Management Strategies or the higher line functions levels can give permission to break a seal.

13.4 If a duplicate key is needed, a written motivation counter signed by the Supervisor should be forwarded to the security component. This will be the case when a member left his/her keys at home.

13.5 The duplicate keys of registries and other sensitive areas have to be stored in a properly sealed envelope (with its details on the outside) by the Key Control Officer in the Section responsible for access control, with proper record keeping. Sealed envelopes are subject to controlling actions by the Information Security Unit while the Office Head can implement measures to his/her satisfaction.

13.6 **Duplicate keys of other offices and buildings.**
Regional Heads employ controlling measures themselves and can give permission for duplicate keys to be released.

13.7 A key control register, has to be filled out for keys of steel and other cabinets, lockable containers etc., and must be controlled by Heads of Office.

13.8 The KCO has to ascertain that duplicate keys are available and safeguarded for every office.

13.9 The KCO will safeguard duplicate keys and the most recent lock combinations, which must remain, sealed in the envelopes in which it has been received. These envelopes are subject to controlling measures by Security and Risk Management/or the client/user Division.

14. COMBINATION SETTINGS OF SAFES, VAULTS AND STRONGROOMS

14.1 Lock combinations of safes, vaults and/or strong rooms must be set by the users and memorized. The combination must be written on an A4-size (folio) paper, folded in such a way that the written numbers are covered on both sides by at least two layer of paper, sealed in and envelope on which the following particulars are displayed:

- the date of sealing by affixing an official date stamp;
- signature of the member(s) sealing the envelope;
- the serial number of the relevant safe/strong room; and
- the number of the office and name of the building in which the relevant safe/strong room is situated.

14.2 The sealed envelope is sealed in a second envelope and sent to the KCO in the Security Component.

14.3 As soon as a new safe/strong room, which uses both a key and combination lock, is put into service, the duplicate key (which takes the place of a combination code setting) is sent to the component responsible for access control. Ensure that the duplicate key and combination code are not put in the same inner envelopes. *Avoid using numbers, which are multiples of 5 and 10. High and low numbers must be alternated and must preferably not be higher than 85 or lower than 15. Do not use combinations that can easily be*

connected or relayed to the user, e.g., birth dates, telephone numbers, vehicle registration number etc.

14.4 The same combination may not be used more than once in any of four consecutive settings.

14.5 Combinations must be memorized by the member and may not be made available to other members who are not co-users. Written notes of the combination are strictly forbidden.

14.6 **Resetting of combinations**

14.7 A combination code will be valid for three (3) months, unless compromise takes place or is suspected of having taken place. On the last working day of such a period, a new code should be introduced. In the case of compromise or possible compromise the combination must be immediately reset.

15. COMPROMISE OF KEYS/COMBINATION

15.1 Compromise should be assumed when:

- the envelope in which a combination or key was sealed is opened or is found open for some or other reason;
- a new combination lock is received;
- a member responsible for a safe or strong room resigns;
- any other circumstances indicate possible compromise.

15.2 Events, which suggest that a compromise has taken place or, even if only such suspicion exits, must be reported as soon as possible to the Security & Risk Management Strategies, as soon as it is suspected or when it comes to attention.

16. REPAIR OF LOCKS/COMBINATION LOCKS AND THE PROVISION OF ADDITIONAL KEYS

16.1. Repair of any lock or the provisioning of an additional key may only be authorized by the component responsible for access control (Security).

16.2 The repair of locks, safes or strong rooms must be undertaken under the auspices of the component responsible for access control, in the case of head office or where applicable, while Heads of Offices elsewhere must take care of supervision.

APPLICATION FORM FOR IDENTITY CARD
OFFICE OF THE PREMIER

PERSONAL DETAILS AND DECLARATION

Title……First Names……
Surname……ID Number…….
SBU/Component……Tel……
……
Cell……..Persal Number……
Office Number……Divisional Head(Initials & Surname)
……
Reason for taking another card……..
……...
……..

Application for: ID Card ☐ **Office Key** ☐
Lost Card No:…… New Card No:……
Lost Key No…… New Key No:…….

Signature Supervisor……Signature Applicant…….
Date…….. Date……..

PAYMENT AUTHORITY FOR THE REPLACEMENT OF LOST CARD

Payment type: Cheque ☐
Cash ☐
Stop order ☐
Amount Paid:……(Rands/Cents)
……..(in words)

Signature Payee……Date……..

Signature Supervisor……Date…….

Signature recipient……Date……

DECLARATION

I declare and warrant that the information on this application form is true, correct and complete and shall form the basis of the identity card to be provided to me. I understand that any misstatement or non-disclosure, which materially lead to, the unlawful act will lead to the disciplinary/legal action.

Applicant signature…….. Date……..