



REFERENCE: DCS 15/1/P
ENQUIRIES: Mr SR George

Head of Department: Premier
Head of Department: Agriculture
Head of Department: Cultural Affairs and Sport
Head of Department: Education
Head of Department: Economic Development and Tourism
Head of Department: Environmental Affairs and Development Planning
Head of Department: Human Settlements
Head of Department: Local Government
Head of Department: Provincial Treasury
Head of Department: Social Development
Head of Department: Transport and Public Works

SECURITY RISK MANAGEMENT CIRCULAR: 6/2012

ACCESS CONTROL DIRECTIVE: CBD BUILDINGS

1. The Department of Community Safety has revisited its Access Control policy in relation to the WCG facilities for which it is mandated to provide access control.
2. Please find attached Access Control Directive applicable at these buildings. A key provision we would like to bring to your attention relates to visitors which are required to be collected and returned to check points by host officials.
3. Should you have any further enquiry in this regard, please do not hesitate to contact Ms K Schumann at Karin.Schumann@westerncape.gov.za.

S R GEORGE
ACTING HEAD OF DEPARTMENT
DATE: 5/10/2012



Western Cape
Government

Community Safety

DEPARTMENT OF COMMUNITY SAFETY
CHIEF DIRECTORATE: SECURITY RISK MANAGEMENT

ACCESS CONTROL DIRECTIVE

MAKING SAFETY EVERYONE'S RESPONSIBILITY

TABLE OF CONTENTS

1. Purpose	2
2. Scope of Application	2
3. Mandate	2
4. Physical measures	2
5. Searching	3
6. After-hours access	4
7. Issuing process of access cards	4
8. Use of access cards	5
9. Visitors	6
10. Misuse of access cards	6
11. Request for access control reports and CCTV Footage	7
12. Criteria for contractors/consultants	7
13. Implementation	8

1. PURPOSE

- 1.1 The purpose of the Access Control Directive is to regulate access control and security related matters for CBD buildings for which the Department of Community Safety is responsible. The directive must be read and applied in conjunction with the Western Cape Government Transversal Security Policy. Access control measures seek to ensure that all persons gaining access to departmental premises are safe, have valid reasons to enter, are entitled and authorized thereto and that the department, its employees, contractors, clients and visitors will not be exposed to any undue danger, risks and breaches of security.

2. SCOPE OF APPLICATION

- 2.1 The provisions of this Access Control Directive are applicable to all staff members and visitors requiring access to WCG buildings within the CBD and any visitors requiring access to premises accommodating WCG departments and for which the department is responsible for in relation to access control.

3. MANDATE

- 3.1 Heads of Department are required to ensure that proper access control measures are implemented.
- 3.2 Heads of Department are required to take such steps as they may deem necessary to safeguard public premises and protect people thereon against dangerous items and or articles.

4. PHYSICAL MEASURES

- 4.1 To give effect to the above all visitors, contractors and staff members associated with the WCG and who require entry to, or exit from WCG buildings may be subjected to random searches. Vehicles (private or government owned) may be searched on entry or when leaving the building occupied by the department (at garages under the control of Security Risk Management). Property, equipment, parcels, documents, etc. can only be removed from WCG premises with the written authorization to do so (Annexure A).
- 4.2 All visitors must report to the reception desks of the Departmental buildings for security personnel to process such visits. Visitors must remain at the reception area from where the host will collect and return the visitors.

- 4.3 All staff members are required to display their access permits in a visible manner when entering Western Cape Government buildings.
- 4.4 Visitors are to be restricted from gaining access to open plan offices and sensitive areas. Hosts receiving visitors are required to exercise access control beyond the security access points.
- 4.5 Officials who elect to bring personal equipment i.e. laptops, cabling, etc. onto Provincial Government premises are required to declare same on entry and to complete the relevant form (Annexure B).
- 4.6 A list of contact numbers of the Chief Directorate: Security Risk Management is attached as Annexure C and provides details of the responsible persons with regard to access control procedures.

5. SEARCH AND SEIZURE

- 5.1 All persons entering a WCG facility are required to disclose at the security check point any dangerous or potentially dangerous item or article he or she may have on his or her person.
- 5.2 All persons entering a WCG facility may be subjected to a search before being granted access to the premises.
- 5.3 Research has shown that the combination of routine and random searching of visitors, contractors and staff members associated with a particular institution makes a considerable contribution in combatting and discouraging theft.
- 5.4 Should any person (official, visitor or contractor) refuse to be searched he/she may be denied access.
- 5.5 Visitors, contractors or staff members found in the unlawful possession of WCG property may be subjected to departmental disciplinary action and/or criminal prosecution.
- 5.6 All dangerous objects found in the possession of visitors, contractors and staff members will be confiscated and based on the risk it holds for the WCG, be dealt with in terms of the Western Cape Government Transversal Security Policy. No firearms will be allowed on any WCG premises.
- 5.7 The search of any person or property must be done with strict regard to decency and privacy and within the confines of the law.

6. AFTER HOURS ACCESS

- 6.1 Should it be required of employees or contractors to work over weekends, such person must be authorized in writing.
- 6.2 Should the need arise for employees to work later than 18:00 during the week, the Security Control Room, except in emergency situations, must be informed by email.
- 6.3 The notification of after hour access must be processed via the Director of the employee(s) concerned and in the case of contractors, the Chief Director of the program involved.
- 6.4 The notification in terms of the above can be forwarded via electronic mail to the Security Control Room. The persons/contractor so authorized must be able to produce a copy of such notice on request by a security officer on patrol duty.

7. ISSUING PROCESS OF ACCESS CARDS

- 7.1 The Access Card Application (Annexure D) is the form to be used when applying for a new access card.
- 7.2 The form must be fully completed and authorised by the applicable SMS member, so as to verify details.
- 7.3 Access will be limited to the specific area and building at which the employee is stationed. Access to other areas and buildings can be requested and is to be supported by the Security Manager of the applicable Department to which access is requested.
- 7.4 All completed and signed application forms must be accompanied by a letter of appointment and a copy of the identity document of the applicant.
- 7.5 All access cards are issued by the Chief Directorate: Security Risk Management. Cards issued as such remain the property of the Department of Community Safety.
- 7.6 Each authorized employee will be issued with one access card except in those instances where more than one access control system is use.
- 7.7 Officials leaving the Public Service for whatever reason must hand their cards over to their respective supervisors on the last day of service. The card must be forwarded to the Chief Directorate: Security Risk Management within 3 days.
- 7.8 Access cards will be deactivated on receipt of the card or after receipt of the monthly Persal termination report by SRM, whichever comes first.

NOTE: Access Cards of contract personnel, who have received extensions to their contracts and the extension does not reflect on the Persal termination report, will be deactivated until such time as the notice of extension is received by SRM.

- 7.9 Should a person be transferred to another Department or building of the WCG, the Director Provincial Security Operations, must be informed by the supervisor in writing thereof within 3 days of the person reporting for duty at the new point.
- 7.10 The access cards of employees are registered at an access point where they are primarily based. Attendance reports are generated in terms of these access points and it is important that supervisors ensure that employees are registered at the correct access point.
- 7.11 The Chief Directorate: Security Risk Management needs to be informed in writing in the event of an employee's name changing to ensure records reflect the correct details of all employees as captured on Persal.
- 7.12 Applications for access cards to the legislature building will be considered after receiving the approved application form from the SA Police Service, stationed at 7 Wale Street.

8. USE OF ACCESS CARDS

STAFF:

- 8.1 The following rules govern the issue and use of access cards of employees:
 - 8.1.1 Each cardholder shall use his/her card every time on entering and exiting an access point. Same will apply in case of biometric finger reader where the index finger is scanned. Pedestrians are not allowed to access a building through a garage.
 - 8.1.2 Under no circumstances are registered users (biometric or card holders) permitted to provide access to another person, swipe for another person and / or allow another person to tailgate at any access point. Persons found to do so compromise the safety and security systems of the WCG and may be subjected to disciplinary action.
 - 8.1.3 Possession of an access card giving legitimate access to a specific area, building or premises does not confer the right to be in any other area, other than as authorized on the card and only when on official business.
 - 8.1.4 Legitimate access to a specific site or area does not confer the right to take unauthorized persons into that building.

- 8.1.5 Access cards must be produced on request by security officials or security personnel contracted to the Department of Community Safety in a security capacity.
- 8.1.6 Lost or stolen access cards must be reported to the responsible official of the Chief Directorate: Security Risk Management as reflected in Annexure D immediately to disable the card. In addition stolen cards must be reported to SAPS.
- 8.1.7 Cardholders will be held responsible for the cost of replacement of lost, stolen or damaged cards occasioned due to negligence.
- 8.1.8 Access cards not in use for a continuous period of 30 days, will be deactivated. Arrangements must be made in writing to inform Security Risk Management in the event of absence longer than 30 days.
- 8.1.9 In the event of an employee, visitor or contractor not returning an access card to Security Risk Management on termination of association with WCG, the cost thereof will be pursued.
- 8.1.10 Lost/stolen access cards will only be re-issued after a receipt of payment for the replacement cost payable at the cashier of Department of Community Safety is produced.
- 8.1.11 Lost cards will only be replaced at no cost to the cardholder if the Director Provincial Security Operations is satisfied that the loss is not due to negligence. A statement is required to support such an application.

VISITORS:

- 8.2. A visitor's access card must be used to give visitors access to the building.
- 8.3 Employees are not allowed to swipe their own cards for visitors.
- 8.4 The security official may issue a visitors card and will allow visitors to enter after they have signed a register and are collected by the host.
- 8.5 Visitors' cards issued must be handed back at the security access point on exiting the building.

9. MISUSE OF ACCESS CARDS

- 9.1 In the event of card misuse, access may be revoked and reported to the applicable Director. It may result in disciplinary action.
- 9.2 The following may inter alia constitute misuse of an access card:

- Lending/borrowing an access card to/of another cardholder/non cardholder.
- Non swiping of access cards without a valid reason.
- Persistent attempts to access non-authorized areas.
- Forcing access where a card will not permit legitimate access.
- Persistent failure to prominently wear/display access cards in the workplace.

10. REQUEST FOR ACCESS CONTROL REPORTS AND CCTV FOOTAGE

10.1 Request for Access Control Reports/CCTV footage

10.1.1 Access reports may be provided on a monthly basis to security managers of departments and on request after a security breach.

10.1.2 CCTV footage can be provided to assist in the investigation of a breach. The breach needs to be reported on the attached form (Annexure E) and forwarded to Security Risk Management with a request for the CCTV footage and access control reports.

10.1.3 Please note that footage is only available for a limited period at this stage due to technical reasons (approximately 30 days). Once requested the footage can be secured for longer periods.

11. CRITERIA FOR CONTRACTORS/CONSULTANTS

11.1 The Head of the unit where the contract/consultant is appointed must furnish a letter to the Director: Provincial Security Operations containing the following information:

11.2 The areas where the contractor/consultants will perform their activities.

11.3 A short description of the task that must be performed.

11.4 The duration, nature and expiry date of the contract.

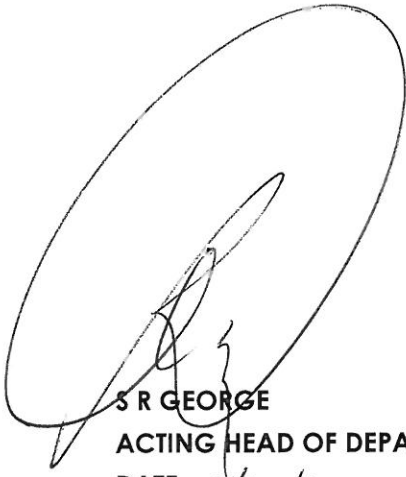
11.5 Full names, surnames and ID numbers must be indicated.

11.6 If it is necessary for contractors/consultants to work outside office hours, the security control room must be informed, in advance (Friday before scheduled work, refer to paragraph 6).

12. IMPLEMENTATION

12.1 This directive is effective immediately and has to be brought to the attention of all employees of the WCG working in the buildings within the CBD.

12.2 Supervisors are required to ensure that the contents of this directive are communicated to all their staff in compliance with the Minimum Information Security Standards (MISS).

A large, handwritten signature in black ink, enclosed within a large, hand-drawn oval. The signature is stylized and appears to read 'S R GEORGE'.

S R GEORGE

ACTING HEAD OF DEPARTMENT

DATE: 5/10/2012



CHIEF DIRECTORATE: SECURITY RISK MANAGEMENT

AUTHORISATION TO REMOVE GOODS FROM WCG BUILDINGS/PREMISES

A. FOR THE USE OF AUTHORISING OFFICER

PERSON AUTHORISED TO REMOVE GOODS

DEPARTMENT: _____

Name: _____

Component/Firm: _____

Persal Nr: _____ Tel/Ext: _____

Access/Visitor's permit No: _____

Reason: _____

SIGNATURE: _____

DATE: _____

DESIGNATION: _____

GOODS Computer

Other equipment

No. of items: _____

Description: _____

Serial No. (where applicable): _____

AUTHORISATION BY

DEPARTMENT: _____

Name: _____

Component/Firm: _____

Persal Nr: _____ Office No.: _____ Tel. No.: _____

Item(s) must be / will not be returned. Date returned: _____

SIGNATURE: _____

DATE: _____

DESIGNATION: _____

B. FOR THE USE OF SECURITY STAFF

I hereby confirm that the above mentioned goods have been removed and verified.

NAME OF OFFICER: _____

DATE: _____

ACCESS POINT: _____

BUILDING: _____

Removal of goods between two buildings: From _____ to _____

SIGNATURE: _____

DATE: _____

TIME: _____



CHIEF DIRECTORATE: SECURITY RISK MANAGEMENT

PROOF OF PERSONAL PROPERTY ON STATE PREMISES

I confirm that the following item(s) is/are my personal property.

Name: _____ Persal number: _____

Department: _____ Office number: _____

Building: _____ Telephone number: _____

Signature of owner: _____ Date: _____

DESCRIPTION	COUNT	SERIAL NUMBER/S

Signature (Security Officer): _____

Name printed: _____

Date: _____

THIS FORM MUST BE HANDED TO SECURITY WHEN LEAVING THE BUILDING

Checked by Security officer: _____

Signature (Security Officer): _____

Name (Security Officer): _____

Date: _____



Directorate: Provincial Security Operations

CONTACT PERSON	SECTION	LOCATION	TELEPHONE	EMAIL
PHYSICAL SECURITY				
Security Control Room	Reporting of emergency/fire /theft/ breaches and after-hours access	Mezzanine floor 4 Dorp Street	021 483 4770 021 483 5555 021 483 6341	HelpSafety.Security@westerncape.gov.za
Nazeem Jaffer: Act DD Physical Security and OHS	Emergency Manager Safety and Security	5 th Floor 35 Wale Street	082 868 3831 021 483 3462	Nazeem.Jaffer@westerncape.gov.za
Edward Patience: ASD: Physical Security	Physical Security Operations	5 th Floor 35 Wale Street	021 483 3942 084 812 1927	Edward.Patience@westerncape.gov.za
Mark Henry: Act ASD: Physical Security Zones	Physical Security Operations	5 th Floor 35 Wale Street	021 483 4775 072 732 4057	Mark.Henry@westerncape.gov.za
FACILITY SAFETY				
Christopher Eksteen: Assistant Emergency Manager	Occupational Health and Safety and Contingency Planning	5 th Floor 35 Wale Street	021 483 2951 074 829 0918	Christopher.Eksteen@westerncap.gov.za
ELECTRONIC ACCESS CONTROL				
Simon Sekwadi: DD Electronic Access Control System	Electronic Access Control System	5 th Floor 35 Wale Street	021 483 8451	Simon.Sekwadi@westerncape.gov.za
Robert van der Westhuizen: ASD	Electronic Access Control: Permit Office (access control: new cards/ replacement cards) Electronic Access control reports	Basement 35 Wale Street	021 483 5525 074 171 3619	Robert.VanDerWesthuizen@westerncape.gov.za
Wajdie Hendricks: Electronic Access Control Administrator	Access Control System & CCTV: requirements, malfunctions Requests for CCTV footage	5 th Floor 35 Wale Street	021 483 6284 079 677 8002	Wajdie.Hendricks@westerncape.gov.za
SAFETY AND SECURITY HELPDESK				
Kenny Robertson	Helpdesk for safety and security matters (malfunction of access control equipment, OHS etc.)	Control Room 4 Dorp Street	021 483 6341	HelpSafety.Security@westerncape.gov.za
Report emergencies to the Security Control Room and the Emergency Manager				

Making safety everyone's responsibility



CHIEF DIRECTORATE: SECURITY RISK MANAGEMENT

SRM 021

APPLICATION FOR WESTERN CAPE GOVERNMENT ACCESS CARD

PERSONAL PARTICULARS

Initial & Surname													
Persal no.													
I.D no.													
Official parking	N/A	Garage (B, C, D, E, ect.) >						Bay no.					
Department							Directorate						

Telephone Ext.				Building:			
I understand the attached terms and conditions in respect of the issue of this card and agree to abide by those conditions.							
Signature:				Date:			

ACCESS PARTICULARS

Building and area where access is required		(Mark X where applicable)	
No. 4 Dorp Street	Turnstiles/		OTHER PREMISES (Note: Indicate the Floor)
	C & D Parking levels/Booth		
	Access Doors: Floors		
No. 9 Dorp Street	Parking levels (G-level)	Waldorf Building	Floor: G,1,6,9,10,11
	Parking levels (F-level)	Norton Rose House	Access Doors – 1 st ,2 nd Flr
	Turnstiles	35 Wale Street	Floor: B/ment,2, 3, 4, 5
	Paraplegic gate	Grand Central	Turnstiles/Access doors
	Access Doors: Floor	PTSS – Athlone	Turnstiles/Floors
Alfred Street	R-parking level	1 & 3 Dorp Street/Leeusig Building	Turnstiles/ Access Doors
	Hospital entrance (CMD)		Paraplegic gate
	Library & Parking entrance		Turnstile/Access Doors
Government Motor Transport (GMT)	Top Yard	Union House (14 Queen Victoria)	Paraplegic gate
	Roeland Street (M/E)		Turnstile
	Hope Street (Workshop)	27 Wale Street (ISM)	J & H & K Parking Levels
	Buitenkant Street (Despatch)		Access door - Floors
Golden Acre	Access Doors	Protea Assurance	Turnstile/Floors
11 Leeuwen Street	Turnstiles/Access doors	142 Long Street	Access Doors
Atterbury House	Access Doors	Alexandra Precinct - Maitland	Access doors

OFFICIAL EQUIPMENT ISSUED TO APPLICANT

Description	Serial Number

APPROVAL BY SMS MEMBER: I hereby certify that the above-mentioned particulars of the employee are correct.

SIGNATURE DESIGNATION TEL. NO. DATE

CONTRACTORS/ CONSULTANTS

FIRM	EXPIRY DATE OF CONTRACT
NATURE OF CONTRACT	

Approval by GWC Contract Administrator: I hereby certify that the above-mentioned particulars of the specified contractor are correct.

SIGNATURE DESIGNATION TEL. NO. DATE



Reference: DCS 15/9/P

ADDENDUM TO APPLICATION FOR WESTERN CAPE GOVERNMENT ACCESS CARD

1. The approval of an application for a WCG Access Card is subject to the following terms and conditions:
 - 1.1 The applicant will familiarize himself/herself with the approved Access Control Directive as circulated by the Department of Community Safety.
 - 1.2 The applicant will take the necessary care and precautions against loss of the access card.
 - 1.3 In case of loss or stolen access permit it is the responsibility of the Cardholder to report such a loss immediately to the following officials within Security Risk Management Robert van der Westhuizen – 021 483 5525/Robert.VanDerWesthuizen2@westerncape.gov.za or Karen Friester 021 483 6284/021 483 5721 /Karen.Friester@westerncape.gov.za
 - 1.4 In the unfortunate event of the applicant being the victim of crime and the access control card is stolen or lost, the loss must be reported to SAPS on the same day when the incident occurred.
 - 1.5 It is also the responsibility of the applicant to report the incident to Security Risk Management on the same day of the incident or on the first working day preceding the incident so as to ensure deactivation of the access control card.
 - 1.6 On the applicant's return to work a copy of the statement made to the SAPS with the details of the incident, case number and a letter requesting the replacement of the access card must be submitted to Security Risk Management (Permit Office – 35 Wale Street, Basement).
 - 1.7 In case of termination of service the official must hand his/her access permit to Security Risk Management permit office on the last working day or his/her supervisor must inform Security Risk Management so that the access permit can be de-activated.
 - 1.8 The official must at all times have his/her access permit available for inspection by an authorized officer. The official permit must always be visible.
 - 1.9 The official must under no circumstances make his/her access permit available to any other person.
 - 1.10 The applicant remains responsible for his/her access card. Lost/stolen/damaged access cards will only be re-issued after a receipt of R112.00 payable at the cashiers on M-Floor at 15 Wale Street (Department of Community Safety), is produced.



Reference: DCS 15/9/P

Acceptance of Terms and Conditions

I acknowledge receipt of card No.: _____

I understand the terms and conditions of issue of this card and agree to abide by those conditions.

Name: _____

Department/
Company: _____

Signed: _____

Date: _____

Noted by: _____

Date: _____



SECURITY BREACH NOTIFICATION

DEPARTMENT		TEL		E-MAIL		OB NR	
INSTITUTION/ BUILDING		FAX		Name of reporting official		SAPS Reported	
BREACH DETAILS / NATURE OF BREACH							
Date and time of Breach	Date reported	Where did breach occur?		Loss of life	Damage of Property	Theft	
	Access control report required			Injuries	Bomb threat	Other	
CCTV footage required		Serial Number / SAPS Case Nr.					
Breach description							
Short description of what happened, only one incident per page							
SECURITY RISK MANAGEMENT PURPOSES ONLY							
Received by & Date Received	CCTV footage supplied	Access control report supplied	Forwarded to SAS	Investigated by	Date Finalized	Date report Submitted	Database Updated