Western Cape Government

Department of Police Oversight and Community Safety

WESTERN CAPE GOVERNMENT: ACCESS CONTROL DIRECTIVE

APPROVALS

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof for and on behalf of the parties represented by them.

Adv K Pillay
Chief Director: Security Risk Management

5/08/2024
Date

Mr H Arendse
Acting Head of Department

Hilton R Arendse
2024.08.28 10:45:48
+02'00'

Date

Title	ACCESS CONTROL DIRECTIVE
Document Owner	**Department of Police Oversight and Community Safety**
Created By	**Security Risk Management**
Date Created	**June 2024**
Electronic file name	**POCS 8/5/P**
Document location	**Department of Police Oversight and Community Safety Main Registry**

Revision History

Revision	Change request	Change comment
0.1	New document	Approved: 6 January 2011
1.0	Revision of document	Approved: 5 October 2012
2.0	Revision of document	Approved: 25 April 2014
3.0	Revision of document	Approved: 23 November 2015
4.0	Revision of document	Approved: 12 May 2016
5.0	Revision of document	Approved: 03 April 2018
6.0	Revision of document	Approved: 18 April 2019
7.0	Revision of document	Approved: 11 December 2020
8.0	Revision of document	

Table of Contents

WESTERN CAPE GOVERNMENT (WCG) VALUES

INTRODUCTION

A system of security measures is essential to create an optimal information security environment. This system naturally is as efficient as its weakest link/element. In this regard, access control and movement control are the links or elements that are prerequisites for an effective security system.

Access control is the process in which several measures are applied to ensure that any object or person requiring access to a Western Cape Government (WCG) premise or an institution, is safe, has a bona fide reason to enter, is entitled and authorized thereto, and that the institution and its staff will not be exposed to danger or breaches of security during the presence of such a person or due to his/her gaining access.

In cases where different WCG departments occupy, use or control different parts of the same building or where different WCG departments occupy, use or control different parts of the same building together with other institutions, consensus between the Heads of Departments and the Heads of other institutions is a prerequisite for the uniform application of the provisions of the Control of Access to Public Premises and Vehicles Act, 1985. Where WCG departments or other institutions apply the provisions of the Act, notices should be displayed to inform members of the public who wish to gain access in a reasonable manner that the Act is being applied.

This Access Control Directive will provide clear direction to help keep WCG employees, visitors etc and property safe. It will indicate various responsibilities as it relates to access control in WCG facilities.

1. PURPOSE

1.1 The purpose of the Access Control Directive is to provide procedures to regulate access control and security related matters at Western Cape Government (WCG) facilities. The directive must be read and applied in conjunction with the Control of Access to Public Premises and Vehicles Act (53/85), the Western Cape Government Safety and Security Strategy and the WCG Security Policy Framework.

1.2 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 Western Cape Government staff members, visitors and contractors who require access to any WCG facility whether in the Cape Metro or elsewhere.

3. DEFINITIONS AND ACRONYMS

Access Control	means the practice of controlling and monitoring access and egress to a property or asset. Access control can be achieved through a combination of manned guarding, mechanical or technical means, access/egress control policies and procedures and asset control policies and procedures.
Authorized officer	means any person authorized by the owner of any public premises or any public vehicle to act in terms of the provisions of section 2 of Act 53/85.
CCTV	means Closed Circuit Television.
Concierge	means a person appointed to welcome and assist visitors to WCG facilities.
Contractor	means a person or firm that undertakes a contract with the WCG to provide materials and/or labour to perform a service for the WCG.
Dangerous Object	means any explosive or incendiary material, any explosive or incendiary device, any firearm, and any gas, material, weapon or other article, object or instrument which may be employed to cause bodily harm to a person, or to render a person temporarily

	paralysed or unconscious, or to cause damage to property, as well as anything which the Minister may by notice in the Gazette declare to be a dangerous object.
Owner of any public premises or any public vehicle	means the head of the department of State, division, office or other body which occupies or uses those premises or that vehicle or is in charge thereof, as the case may be.
Physical Security	means the use of physical measures to prevent and delay unauthorized intrusion and to protect assets and personnel.
POCS	means the department of Police Oversight and Community Safety.
Public premises	means any facility, structure, hall, room, office, convenience, land, enclosure or water surface, which is the property of, or is occupied or used by, or is under the control of, the State or a statutory body, and to which a member of the public has a right of access or is usually admitted or to which he may be admitted.
Risk	means the likelihood of a threat materializing by exploitation of an event or incident to create vulnerability.
SAPS	means the South African Police Service.
SAS	means Security Advisory Services.
Security Manager	means the WCG employee appointed by his/her respective Head of Department to manage security related functions with his/her department.
SOP	means Standard Operating Procedure
SRM Forms	forms are available on the WCG website.
SRM 001	Removal Form
SRM 002	Personal Property on State Premises
SRM 003	Application for Access Card - Legislator Building
SRM 004	Application for Access Card - Legislator Building 1st Floor
SRM 014	Prohibited Items
SRM 021	Application for WCG Access Card
SRM 022	Staff No Card Register
Visitor	means a person who visits the WCG facilities for reasons of friendship, family, business, duty, or the like.
WCG	means the Western Cape Government.

WCG Facilities	means all facilities owned by or a private facility leased/partially leased by the WCG.
WCG Staff	All persons employed by the WCG, including Senior Managers, Middle Managers, contract employees and interns.

4. LEGISLATIVE FRAMEWORK

4.1 The following legislation and policies regulate access control at WCG facilities:

4.1.1 The Control of Access to Public Premises and Vehicles Act 53 of 1985

4.1.2 Minimum Information Security Standards of 1996

4.1.3 Minimum Physical Security Standards

4.1.4 Protection of Personal Information Act 4 of 2013

4.1.5 Cabinet Memo 273/2005

4.1.6 Criminal Procedure Act 51 of 1977

4.1.7 Private Security Industry Regulation Act 56 of 2001

4.1.8 Firearm Control Act 6 of 2000

4.1.9 Occupational Health and Safety Act 85 of 1993

4.1.10 WCG Security Policy Framework

4.1.11 Disaster Management Act 57 of 2002

5. LEGISLATIVE MANDATE

5.1 Section 2 (1) of the Control of Access to Public Premises and Vehicles (Act 53/1985) mandates the owner of any public premises or any public vehicle, to:

5.1.1 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.

5.1.2 Direct that those premises or that vehicle may only be entered or entered upon in accordance with the provisions of sub-section (2).

5.2 Cabinet Memo 273/2005 authorised the establishment the programme Security Risk Management (SRM) within the Department of Police Oversight and Community Safety with the purpose of the transversal management and oversight of security and related functions on behalf of all HODs of the Western Cape Government.

5.3 Memo 273/2005 further authorised the establishment of the Directorate: Provincial Security Provisioning; mandated to enhance safety and security provisioning through the development, implementation and maintenance of operational security methodologies and processes.

6. METHODOLOGIES AND PROCESSES

To give effect to its mandate, the Directorate: Provincial Security Provisioning has developed the following access and egress control methodologies and processes, applicable to all WCG employees, visitors and contractors at WCG facilities.

6.1.1 PHYSICAL SECURITY MEASURES

IMPORTANT:

WCG staff must always wear and visibly display their WCG access cards and must identify themselves when requested to do so by security.

6.1.2 VISITORS:

The provisions applicable to visitors stated below will also be applicable to a WCG staff member who does not have authorized electronic access to a specific WCG facility.

PROCESS TO BE FOLLOWED:

a) All visitors and contractors must report to the reception desk of the WCG facilities to which access is required, to enable the security personnel to process such visits.

b) Once processed, visitors will be issued with a visitor's sticker, which must always be displayed whilst in the WCG facility.

c) Visitors and contractors must declare if they are in possession of any dangerous weapon(s) and personal electronic or other devices.

d) The WCG staff member associated with the visitor or contractor must collect such a visitor or contractor at the reception desk of the facility.

e) At the conclusion of the visit, the respective WCG staff member must escort his/her visitor back to the reception desk of the WCG facility.

f) Visitors and contractors must remain in the reception area of the respective WCG facility until such time that they are met by their respective host.

g) The host receiving visitors or contractors is required to exercise control of their visitors or contractors beyond the security access points.

h) Visitors are to be restricted from gaining access to open plan offices and sensitive areas.

i) All visitors must return visitor stickers to the security official when leaving the facility at the main entrance.

j) The above-mentioned process is also applicable to those visitors and contractors who have received prior authorisation to utilise one of the official vehicle parkade's, associated with the WCG.

6.1.3 CONTRACTORS

6.1.3.1 Should a department make provisions for contractors to be on a WCG site or building, arrangements must be made by the Facility Manager through the WCG department's Security Manager to the WCG Security Control Room at 021 483 4770/5555 or SRM.controlroom@westerncape.gov.za and the Safety & Security helpdesk helpsafety.security@westerncape.gov.za.

6.1.3.2 To assist with operational planning, where possible, these arrangements must be made three (3) working days before the contractor arrives. Contractor access and egress will be in accordance with the Contractor Escorting Standard Operating Procedure (SOP).

6.1.4 SAPS CLEARANCES

6.1.4.1 All employees of contracted services must be subjected to a SAPS clearance.

6.1.4.2 It is the responsibility of the respective departmental Security Manager to ensure and confirm that all employees of contracted services have been subjected to a SAPS clearance. This confirmation must form part of the request for access to perform contracted work and must be submitted through the helpdesk official email address helpsafety.security@westerncape.gov.za

6.1.5 USE OF MASTERCARDS

The use of Mastercards must be limited to extra ordinary situations and may only be used by security personnel in accordance with the developed Standard Operating Procedure.

6.1.6 SEARCHING

6.1.6.1 All WCG staff, visitors and contractors associated with the WCG who require entry to/or exit from WCG facilities may be subjected to random searches in terms of the Control of Access to Public Premises and Vehicles Act, 1985.

6.1.6.2 All searching at WCG facilities must be conducted in accordance with Section 29 of the Criminal Procedure Act 51 of 1977.

6.1.6.3 Vehicles (privately owned or government) may be searched on entry or when exiting a WCG facility.

6.1.6.4 No dangerous objects are allowed in WCG facilities and as such all persons requiring access to a WCG facility must declare the presence of such to the security.

6.1.6.5 Any WCG staff, visitor or contractor found in possession of dangerous objects will be refused entry, until such time that the WCG staff member, visitor or contractor has safely disposed of such in a lawful manner.

6.1.6.6 Searching of WCG staff, visitors and contractors will be conducted with hand-held or walk-through metal detectors.

6.1.6.7 Parcels and handbags must be searched in the presence of the owner and with the utmost care to prevent damage to and contact with personal items.

6.1.6.8 Persons with pacemakers are excluded from being scanned with a metal detector. In this regard a letter from a medical practitioner can be provided to the WCG Access Control Permit Office, situated at 35 Wale Street, to capture such exclusion on the respective staff member's access card.

6.1.6.9 Property, equipment, parcels, documents, etc. can only be removed from WCG facilities with the written authorisation from the respective security manager or the person delegated by the security manager to provide such authorisation **(SRM 001).**

6.1.6.10 Officials who elect to bring personal equipment i.e., laptops, cabling, etc. into WCG facilities are required to declare same on entry and to complete the relevant security authorisation form **(SRM 002).**

6.1.6.11 This written authorisation **(SRM 001** or **SRM 002)** must be presented to the security official on exit of the WCG facility.

6.1.6.12 Should any WCG staff member, visitor or contractor refuse to be searched, access to the WCG facility will be denied. The refusal will be reported to the relevant supervisor of the WCG staff member or the WCG staff member associated with the visitor or contractor.

6.1.6.13 Visitors, contractors or WCG staff members found in the unlawful possession of WCG property may be subjected to departmental disciplinary action and/or criminal prosecution.

7. FIREARM/DANGEROUS OBJECTS

7.1 Section 1 (a)(ii) of the Control of Access to Public Premises and Vehicles Act (1985), defines a Dangerous Object as being "any explosive or incendiary material, any explosive or incendiary device, any firearm, and any gas, material, weapon or other article, object or instrument which may be employed to cause bodily harm to a person, or to render a person temporarily paralysed or unconscious, or to cause damage to property, as well as anything which the Minister may by notice in the Gazette declare to be a dangerous object for the purposes of this Act".

7.2 Section (2)(1)(a) of the Act, stipulates that, the owner of any public premises or any public vehicle may "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."

7.3 In accordance with the Act any person(s), including WCG staff members, requiring entry to a WCG facility will be required to declare if he/she has any dangerous object in his or her possession.

7.3.1 Should the declaration be positive, the person requiring entry will be informed that dangerous objects are not permitted in WCG facilities.

7.3.2 Permission to enter a WCG facility will be denied until such time that the person requiring entry has removed the dangerous object from the WCG facility.

7.4 In accordance with Section 3 of the Act, the requirements mentioned under paragraph 7.3, 7.3.1 and 7.3.2 are not applicable in respect of any member of a police force established by or under any law, including members of the South African Police Service, Metro Police and Law Enforcement officials or a member of the South African Defence Force who is required in the performance of his functions to enter or enter upon any public premises or public vehicle and who produces proof of his identity to the satisfaction of the authorized officer concerned.

7.5 WCG Departments firearm management processes must comply with all relevant legislative prescripts including the Control of Access to Public Premises and Vehicles Act, 1985 and/or the Firearm Control Act, Act 6 of 2000.

8. SAFETY AND SECURITY HELPDESK

8.1 The Safety and Security helpdesk aids in improved communication as a rapid response system in the management of access control activities.

8.2 All access control requirements must be channelled through the respective departments' Security Manager to the Safety and Security helpdesk at helpsafety.security@westerncape.gov.za.

8.3 It is important that all faulty access control equipment be reported to the safety and security helpdesk immediately. This will maximise the system in reducing risk.

8.4 Malicious damage to the access control system will be for the account of the department concerned.

8.5 Access doors are linked to an alarm system in the WCG Security Control Room and as such, all access-controlled doors must be kept closed at all times. If doors are being

kept open for longer than 15 seconds, it results in alarm flooding and the system malfunctioning.

9. APPLICATION FOR ACCESS

9.1 All applications for temporary and/or permanent access to a WCG facility or specific area within a WCG facility is done by completing the prescribed Application for Western Cape Government Access Card **(SRM 021).**

9.2 All applications for temporary and/or permanent access to the Western Cape Provincial Parliament (WCPP) or specific area within the WCPP is done by completing the prescribed Application for Access to the Legislator Facility **(SRM 004).**

9.3 All applications for temporary and/or permanent access to a WCG facility or specific area within a WCG facility, or the Western Cape Provincial Parliament (WCPP) or specific area within the WCPP, must be channelled via the respective Security Manager, through the applicable SRM: SAS Liaison Officer to the Safety and Security Helpdesk.

9.4 The Safety and Security Helpdesk will acknowledge the activation of the access card via the same communication channel.

9.5 All access cards are issued by the Chief Directorate: Security Risk Management and remain the property of the Department of Police Oversight and Community Safety.

9.6 All WCG employees performing their daily function in a WCG facility situated in the Cape Town CBD will be issued with one (1) official WCG Access Card.

9.7 Officials leaving the employ of the WCG, for whatever reason, must hand their access card to the respective Security Manager on the last day of service. Departments are encouraged to institutionalize this as part of the employee exit interview process.

9.8 It remains the responsibility of the exiting employee to ensure that his/her departure is brought to the attention of his/her respective Security Manager to arrange for the deactivation and handing in of the card. Failure to do so, may result in the fraudulent use of the individual's access card.

9.9 In addition, the CSC is required to provide a Persal termination report to the Safety & Security helpdesk on the 1st of every month. The access cards of WCG employees will be deactivated on receipt of the Persal report or the notification by the Security Manager, whichever is received first.

9.10 Access cards and biometric access that are inactive for a continuous period of 60 days, will be deactivated automatically. Arrangements in terms of absence longer than 60

days, must be made in writing, via the applicable security manager and SRM: SAS liaison with the Safety & Security helpdesk.

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 the Safety & Security helpdesk.

9.11 Should a person be transferred to another Department or facility of the WCG, the Safety & Security helpdesk must be informed in writing by the supervisor via the same communication channel, noted above, within 3 days of the person reporting for duty at the new point.

9.12 WCG access cards are activated to allow individual access by WCG employees to their respective work areas. When requested, attendance reports are generated in terms of these access points and as such it is important that supervisors ensure that their respective subordinates are registered at the correct access point.

9.13 To ensure data integrity, cardholder reports, including a list of all users assigned to the applicable WCG facility or area, are provided to the respective Security Managers on a quarterly basis.

9.14 Security Managers must interrogate these reports for relevance and authenticity and provide details of discrepancies to the Safety & Security helpdesk.

9.15 Unless authorized to use a parkade, no WCG employee may enter any WCG facility through such a parkade, on foot or otherwise.

9.16 Official equipment (laptops etc. indicating serial number) issued to an access card holder for official use, can be registered on the back of the access card of WCG staff for authorised removal from WCG premises. The signed approved **SRM 001** form must accompany this registration which can be submitted to the Permit Office for processing.

10. AFTER HOURS ACCESS

10.1 Authorized access is provided from 06:00 to 18:00 to all qualifying WCG employees.

10.2 Should it be required of employees or contractors to work over weekends and/or later than 18:00, written authorisation must be provided by the respective Security Manager.

10.3 Employees and/or contractors must, upon request, present a copy of the authorisation to security.

10.4 Security Managers must inform the WCG Security Control Room at 021 483 4770/5555 or SRM.controlroom@westerncape.gov.za and the Safety & Security helpdesk helpsafety.security@westerncape.gov.za.

10.5 WCG employees who require 24/7 access must request approval for such in writing though their respective Security Managers to the Safety & Security helpdesk. Approval for such will only be granted in exceptional circumstances and on recommendation from the applicable Security Manager.

11. USE OF ACCESS CARDS BY WCG STAFF

11.1 WCG staff must always visibly display their WCG access cards when on WCG property. Access cards must be produced on request by security officials or security personnel contracted to the Department of Police Oversight and Community Safety.

11.2 Each cardholder shall always use his/her card when entering and exiting an access point. The same will apply in the case of a biometric finger reader where the index finger is scanned.

11.3 Under no circumstances may WCG staff provide access to another person, swipe for another person, allow another person to use his/ her WCG access card and/or allow another person to tailgate at any access point.

11.4 Persons found to do so compromise the safety and security systems of the WCG and may be subjected to disciplinary action.

11.5 Being in possession of a WCG access card that provides legitimate access to a specific area, facility or premises does not confer the right to be in any other area, other than as authorized. Such authorisation is only applicable when the relevant WCG employee is on official business.

11.6 Having authorized access to a specific facility and/or area does not confer the right to take unauthorized persons into that facility and/or area.

11.7 Lost or stolen WCG access cards must be reported to the Safety & Security helpdesk (helpsafety.security@westerncape.gov.za) immediately, so as to ensure the WCG access card is disabled.

11.7.1 In addition to the above, stolen and lost WCG access cards must be reported to the South African Police Service.

11.7.2 WCG employees may be liable for the replacement cost of lost or stolen access cards. Lost or stolen cards will only be replaced at no cost to the cardholder if the Director: Provincial Security Provisioning is satisfied that the loss is not due to negligence by the applicable WCG employee.

11.7.3 A sworn statement is required to support an application for cost deferral.

11.7.4 If the WCG official is liable for payment, a replacement WCG access card will only be re-issued on the receipt of payment for the replacement. Payment can be made at

the cashier of Department of Police Oversight and Community Safety; 4th Floor; 35 Wale Street Cape Town.

11.7.5 An employee will be given a grace period of 3 days to apply for a replacement access card after such a loss, during which time the employee must manually sign the applicable register available at the security check point.

11.8 In the event of an employee, visitor or contractor not returning a WCG access card to Security Risk Management on termination or association with WCG, the cost thereof will be pursued.

12. PARKING GARAGES

12.1 Only persons authorized and allocated an official parking bay, by the Department of Infrastructure, Property Management, may enter the WCG garage to which they have authorization.

12.2 Any person wanting to use the parking bay of a person authorized to park within the garage, must be in possession of written letter of consent from the official indicating the bay number and duration of parking. This letter must be sent to the Permit Office who will grant temporary access to the staff member as per the dates on the authorization letter. The process is summarized below:

12.2.1 The individual obtains permission from the owner of the parking bay. An email would suffice stating the individual's name and surname including the beginning and end date of the temporary parking arrangement).

12.2.2 The authorization is sent via the security manager to the Safety and Security helpdesk prior to the parking date to ensure access is granted timeously.

12.2.3 The temporary access is loaded to the new parking officials' access profile as per the specified dates.

12.2.4 The temporary access will automatically be activated and deactivated based on the dates entered into the system.

12.3 Communication should be sent to the Security Helpdesk (helpsafety.security@westerncape.gov.za) a day before parking is used to ensure security at the parking garage is timeously informed and to avoid not being allowed access to park.

13. MISUSE OF ACCESS CARDS

13.1 In the event of card misuse, access may be revoked and reported to the applicable manager. It may result in disciplinary action.

13.2 The following may inter alia constitute misuse of an access card:

13.2.1 Lending and/or borrowing a WCG access card to another WCG employee or visitor to enter an access-controlled area.

13.2.2 Failure to use a WCG access card to enter an access-controlled area, without a valid reason.

13.2.3 Persistent attempts to access non-authorized areas.

13.2.4 Forcing access where a WCG access card will not permit authorized access.

13.2.5 Persistent failure to prominently wear and/or display WCG access cards in the workplace.

13.3 The use of access cards must be in accordance with the conditions of the signed application for access cards.

13.4 To avoid unauthorized access or cards being used fraudulently, lost cards must be reported immediately and where the loss was due to staff own negligence, payment for a new card must be made and submitted with a new application to the Permit Office.

14. REQUEST FOR ACCESS CONTROL REPORTS AND CCTV FOOTAGE

14.1 While POCS in compliance with POPIA, undertakes to ensure that appropriate security control measures are implemented to protect all personal information against loss, unauthorized access, use, modification, disclosure, or misuse, WCG Departments must develop their own internal POPIA Policy on how to deal with the personal information contained in access reports.

14.2 Access reports and CCTV footage, to investigate breaches or assist in disciplinary investigations, must be requested via the respective Security Managers of departments and the applicable SRM liaison officer to the Safety and Security helpdesk at helpsafety.security@westerncape.gov.za.

14.3 No requests to view CCTV footage to find lost or misplaced personal items will be processed by the Safety and Security helpdesk.

14.4 Requests for CCTV footage and/or access reports to be used as evidence or whilst investigating labour relations matters, must be directed through the applicable Security Manager.

14.5 Due to the sensitive nature of labour relations investigations, the requested footage will be supplied directly to the applicable labour relations official.

14.6 Please note that footage is only available for a limited period of 30 days. Once the request is received by the Safety and Security helpdesk the footage will be secured on

a laptop at SRM. The applicable Security Manager or labour relations officer will be notified of its availability and arrangements for viewing will be made with him/her.

14.7 CCTV footage requested by the SAPS as part of a criminal investigation will be subject to the approval of the Director: Provincial Security Provisioning.

14.8 Access reports and CCTV footage will only be made available to authorized persons, as determined by the applicable WCG internal POPIA policy prescripts. In this regard, Security Managers must provide the Safety and Security helpdesk of the names of such authorized persons and any amendments to such authorizations.

14.9 Access control reports can be used by respective Departments for the purpose of time management should their internal policy reflect such.

14.10 Queries and complaints with regards to access reports and CCTV footage can be sent to HelpSafety.Security@westerncape.gov.za

15. FAULT REPORTING: WCG ELECTRONIC ACCESS CONTROL AND CCTV SYSTEMS

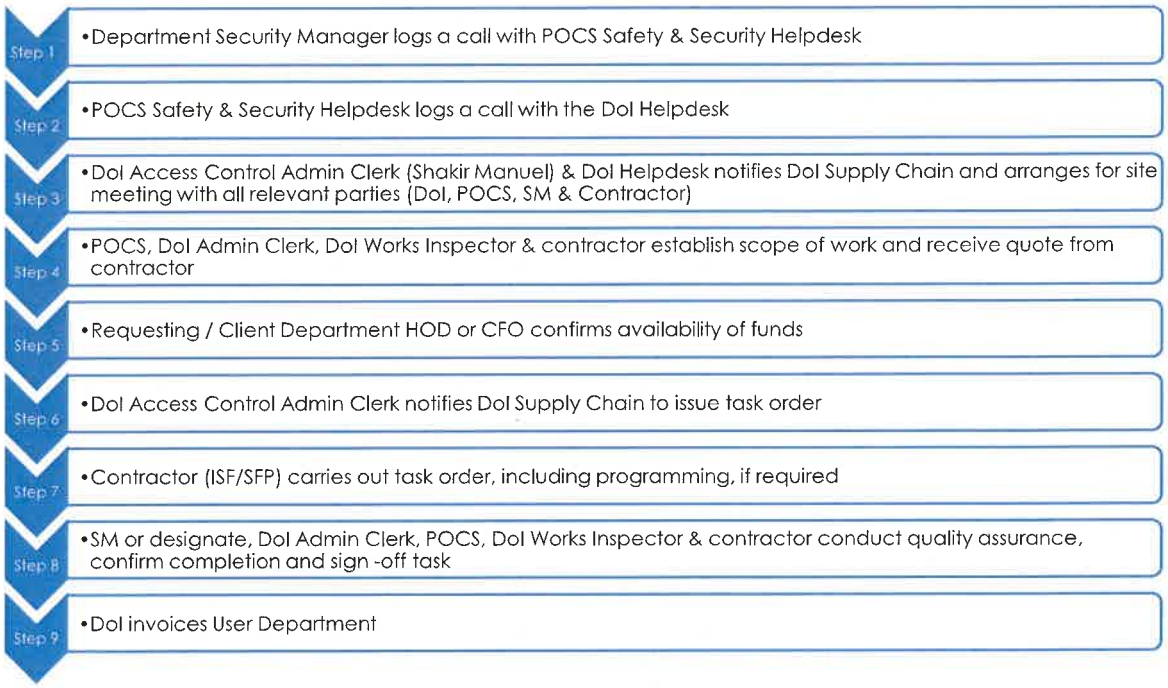
15.1 All defective access control and CCTV equipment at WCG facilities managed by POCS, must immediately be reported to helpsafety.security@westerncape.gov.za to action the repair and/or replacement of defective electronic access control and CCTV equipment in conjunction with the Department of Infrastructure.

15.2 Where possible, POCS may provide loan equipment (like controllers, card readers, recorders, etc.) to departments where access control equipment is damaged beyond repair to ensure adequate electronic access control and that WCG facilities are left vulnerable.

15.2.1 This loan equipment, if compatible with the version installed on the access control system, will be provided for a maximum period of 30 working days to allow departments to procure the replacement through the Department of Infrastructure by using their respective internal procurement procedures. Should it be required, POCS can provide the specifications for the equipment to be procured. For the Qognify Smart Video Recorder (SVR), as it is an international product, the duration will be 90 working days and the same conditions will apply as explained above.

15.2.2 Departments are encouraged to initiate the procurement process as soon as possible in order to ensure all areas remain secured within the mentioned working day period. Should the Department fail to procure new equipment within the specified periods, POCS will initiate the procurement process, on behalf of the procuring department, with the Department of Infrastructure.

15.2.3 The following schematic provides and overview of the process to be followed by WCG Departments should the need arise to procure new access control or CCTV equipment.



16. IMPLEMENTATION

16.1 This directive is applicable to all permanent, temporary and contract staff associated with the WCG, including contractors, visitors and ministry staff.

16.2 This directive is effective immediately and must be brought to the attention of all employees of the WCG.

16.3 Supervisors are required to ensure that the contents of this directive are communicated to all their staff.

16.4 As part of the implementation of this directive and to ensure this access control directive is being followed, WCG Departments with the assistance of POCS will need to conduct regular audits or access permit verifications.

16.5 Any request for assistance with access control audits and permit verifications can be done through the Security Manager to POCS Security Liaison Officers.

17. REVIEW OF GUIDELINE

17.1 The directive will be subject to regular review to ensure its relevance. Feedback from the Departmental Security Managers will inform the necessary revisions and improvements.

Document enquiries can be directed to:

Department of Police Oversight and Community Safety, Western Cape Government, 35 Wale Street, Cape Town, 8000, SA

Attention Mr. Fred Watkins

Designation Director: Provincial Security Provisioning

Email Fred.Watkins@westerncape.gov. za

Telephone +27 (021) 483 8461

www.westerncape.gov.za