Western Cape Government
Community Safety

ANNEXURE 1

Chief Directorate: Security Risk Management

ACCESS CONTROL STANDARD OPERATING PROCEDURE

1. PURPOSE

1.1 To provide a standard operation procedure to regulate access control in WCG buildings in the CBD.

2. METHODOLOGY

2.1 To create resilient institutions in the face of threats which are uncertain an effective security system is needed of a combination of physical barriers, manned guarding, electronic systems, CCTV surveillance and an internal toolset to manage performance of guarding service.

2.2 The Standard operating procedure must be read in conjunction with the Access Control Directive and provide for the procedures to be followed to regulate access of visitors, contractors and staff members to WCG buildings.

2.3 A Safety and Security Helpdesk has been established as an incident management system where all access control matters can be logged and serve as a rapid response system to ensure that faulty access control systems are restored to full functionality and that related security matters are prioritized and speedily resolved.

2.4 The Helpdesk has a dedicated email and telephone number (Helpsafety.Security@westerncape.gov.za /021 4836991) and all access related enquiries are channeled through the helpdesk, i.e. application for access, reporting of faulty equipment, request for CCTV footage, request for access control reports etc.

3. PHYSICAL MEASURES

3.1 To ensure effective control of Access to WCG buildings security officials have to follow certain protocols to ensure a standardised approach in regulating access. The following SRM forms and registers are completed in this regard:

3.1.1 Property, equipment, parcels, documents etc. can only be removed from WCG premises with the written authorization to do so. Form SRM 001 (Annexure A) needs to be completed and produced at the security desk to allow for the removal of the item. Staff can apply to display the details of their equipment on the back of their access cards to ease the process of removal. Applications in this regard can be made through the Departmental Security Manager to the permit office.

3.1.2 Officials who elect to bring personal equipment onto WCG premises are required to declare same on entry and to complete Form SRM 002 (Annexure B).

3.1.3 Contractors have to complete form SRM 017 (Annexure C) to gain access to the building. See paragraph 4 for automated access.

3.1.4 A key register form SRM 015 (Annexure D) has to be completed when keys are collected from the security desk.

3.1.5 Staff that has approval to enter the building after hours is required to complete SRM 020 (Annexure E) to gain access to the building.

4. SEARCH AND SEIZURE

4.1 All persons entering WCG premises must disclose at the security check point any dangerous or potentially dangerous item or article they may have on their person. The person must be asked if they have anything to declare and if in possession of such an item it must be handed over to a security official, the required particulars have to be entered into a dedicated register and locked in a cabinet or other safe place until the time when it is handed back to the person on his/her departure.

4.2 The WCG buildings are gun free buildings and no fire arms are allowed on the premises and cannot be handed in for safe keeping. Only law enforcement agencies on official duties will be allowed to carry fire arms when entering the building.

5. SEARCHING PROTOCOL

5.1 All persons entering a WCG building may be subjected to random searching before being granted access to the premises and will be required to enter via a walk through metal detector or alternatively scanned with a metal detector for dangerous objects.

5.2 Persons with pacemakers will be excluded from being scanned with a metal detector to avoid possible interference with the pacemaker. In this regard a letter from the medical practitioner must be provided to security or alternatively it can be provided to the Permit Office to capture such exclusion on the access card.

5.3 Please note random searching means there is no specific pattern that can be associated with the way searches are conducted.

5.4 Searching of any property or person is being done with strict regard to decency and privacy within the confines of the law, i.e. a female can only search a female and male can search a male. Should any person refuse to be searched he/she may be denied access. Any deviations in this regard should be reported to the security manager to deal with it accordingly.

5.5 The person being searched must be requested in a polite manner to open their bags and security will check the bags. The person must open his/her bag themselves and security is not allowed to put hands in the bag or do a physical body search. The bag must be checked for items that need authorisation to be removed. These items include inter alia computer equipment, cameras, portable hard drives, video cameras etc.

5.6 All vehicles leaving the parking garage must be searched. The driver must be requested to open the trunk of the vehicle/bag themselves and it must be checked for items that need authorisation to be removed.

6. SECURITY RISK MANAGEMENT (SRM) HELPDESK

6.1 FAULTY EQUIPMENT IDENTIFICATION AND REPORTING

6.1.1 Faulty equipment is reported to the helpdesk per email and logged on the database with a reference number that is supplied to the client after it was reported to *the* service provider.

6.1.2 The helpdesk operator must log daily onto the Access Control and CCTV systems to determine all preliminary faults and communicate with the building security and the security manager of the department to alert them of the faulty equipment.

6.1.3 The helpdesk will communicate with the client to report back in the event that the service provider is unable to fix it within the stipulated period. Progress on the resolution of each call logged must be followed up and progress documented until it has been finalised within the specific time period allocated to it. Weekly reconciliation must be done to ensure that all calls have been attended to and the equipment restored to full functionality.

6.1.4 The service provider must inform helpdesk per email when the fault is fixed it will be logged as finalised on the helpdesk and the client informed accordingly. If there are still problems then the client must report it to the helpdesk for further follow up.

6.1.5 After hours faulty equipment to be identified by the Security Control Room with email to helpdesk and official on standby to be informed telephonically in case of an emergency. The official on standby will assess the situation and respond accordingly.

6.1.6 Faulty equipment is prioritised in high, medium and low priority according to the urgency of restoring the equipment.

6.2 APPLICATION FOR ACCESS CARDS BY STAFF AND CONTRACTORS

6.2.1 Applications for access are sent per email to the helpdesk by the applicant after the approval documents have been completed and approved by the security manager of the department. Applications can also be submitted to the Permit office per hand. The applicant will be contacted by the Permit office to set up an appointment for the processing of the application, i.e. registering of fingerprint, identity photo and issuing of an access card.

6.2.2 The Permit office operating hours are 09:00-12:00 and from 14:00-15:00. The following documentation is needed to process an application for access:

6.2.3 Form SRM 021 (Annexure F) approved by the Departmental Security Manager together with a copy of identity document and appointment letter for access to CBD buildings (excluding Legislature Building).

6.2.3 Form SRM 004 (Annexure G) for the Legislature Building approved by the Departmental Security Manager and SAPS together with a copy of identity document and appointment letter.

6.2.4 The fixed period of a contractor appointment is captured on the database when access is given to automatically deactivate the contractor access on the last day of the contract. A letter from the company confirming employees that need access and letter from DTPW appointing the company in terms of the tender.

6.2.5 Any card/biometric access related problems can be emailed to the helpdesk for investigation and rectification.

7. ACCESS FOR VISITORS

7.1 Visitors must report to the security desk with proof of identity at the entrance of a building and will be registered on the electronic visitor management system (VMS) or alternatively a visitors register will be completed by the security official after the visitors identity is checked against a valid identity document (SA identity document/passport/drivers licence). The particulars must be completed in the visitors register (Form SRM016) by the security official as reflected in Annexure H. The host will be contacted by security and the host will collect the visitor from the security desk.

7.2 Visitors can also be identified through personal identification by the host in the event where the abovementioned documents are not available for identification in which case the details of the visitor and the host are recorded in the register/VMS.

7.3 If the visitor is registered on the electronic VMS then the visitor will be issued with a visitor's access card that will give access to the building and distinguish the visitor from staff. The same details as reflected in the manual register will be entered in the VMS and a photo will be taken of the visitor. A time period for the visit is allocated on the system and the system will raise an alarm if the visitor is not out of the building by the stipulated time. The visitor must return the access card in the drop box at the original point of entry to exit the building.

7.4 A visitors report will be extracted from the VMS with the details of visitors that entered and exited the building. Security will collect the cards from the drop box and reconcile the cards with the visitors report to ensure that all visitors have left the building as registered on the VMS.

7.5 Bi-weekly spot checks must be conducted by the security supervisor to ensure that the manual visitor's registers are completed correctly and that visitors are managed effectively. Once the visitor management system has been implemented completely, automated bi-weekly reports will be extracted from the system and analysed to ensure that visitors are managed effectively.

7.6 Staff that do not have access cards are required to be entered into the visitors register (SRM 016) or the VMS system.

8. TERMINATION OF ACCESS

8.1 The SRM helpdesk must be notified per email of the employee's last day of service by the security manager as per internal exit interview protocols of departments to ensure deactivation on the system before the exit of the employee. The deactivation will be programmed on the system accordingly to ensure that the card is deactivated on the last day of service.

8.2 The access card needs to be handed to the security manager on the last day of service and the cards returned to the permit office within 5 days. Reconciliation will be conducted with the Persal termination report within 5 days of receipt of the report to ensure that employee's cards have been deactivated and the cards handed in.

9. AFTER HOURS ACCESS

9.1 When a contractor wants to work in the building after hours or over weekends then prior arrangements should be made with the Control Room by providing details per email of the names and copies of identity documents of the contract people that are required to work.

9.2 The notification of after hour access must be processed via the Security Manager and can be forwarded via electronic mail to the Security Control Room (Xenophone.Wentzel@westerncape.gov.za).

9.3. The persons/contractor so authorized must be able to produce a copy of such notice on request by a security officer on patrol duty.

10. REPLACEMENT OF CARDS

10.1 If the card is stolen or lost in the event of the cardholder being a victim of crime, the loss must be reported to the helpdesk and SAPS by the cardholder. A copy of the statement made to SAPS with the details of the incident, case number and a letter requesting the replacement must be submitted to the permit office for replacement of the card at no cost. Lost 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. A statement is required to support such an application.

10.2 Lost/damaged 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. The permit office will inform the cardholder what the applicable cost is attached to the replacement of the card and payment can be made in cash or by debit/credit card at the cashier's office on the 4th floor at 35 Wale Street. The card will only be reissued after all processes have been completed.

10.3 The cardholder remains responsible for his/her access card and for the deactivation of the card if it is lost or stolen as the card can be used fraudulently.

11. ACCESS AUDIT

11.1 A cardholder report of primary and secondary access to a building will be provided to departmental security managers on a quarterly basis as a tool to audit the system for integrity of data and to restrict unauthorized access.

11.2 The security manager/delegate verifies that the access of the cardholders is correctly reflected on the report or amended report accordingly and returns report to helpdesk for capturing on the system. The reconciled returned cards will also be reported to the security manager with an indication of outstanding access cards, if any.

12. CCTV FOOTAGE AND ACCESS REPORTS

12.1 Access reports and CCTV footage are valuable tools for the investigation of a breach and can be provided if the following process has been followed:

12.1.1 The breach/incident needs to be reported on Form SRM 018 (Annexure I) by the security manager and submitted to the helpdesk/SRM facilitator for investigation of the breach. The helpdesk will provide the access report to the facilitator and secure the CCTV footage on a CCTV workstation at 35 Wale Street within 48 hours. The footage and access reports can only be provided once all processes have been followed to ensure that the investigation is dealt with confidentially and the liaison officer approved the release thereof.

12.1.2 The helpdesk will log the request in the CCTV footage register and provide a reference number to the client. Sufficient information needs to be supplied in terms of the timeline of the footage required to facilitate speedy retrieval of the footage. The CCTV register log the viewing and release of the footage in a secure manner.

12.1.3 An appointment will be set up with the security manager to view the footage at 35 Wale Street. A confidentiality agreement needs to be signed before the footage can be viewed or released to the security manager/delegate.

12.1.4 The downloaded footage will be kept by SRM for 6 months. Should evidence be required by the courts in criminal proceedings/disciplinary hearing a dedicated portable viewing unit is available to display CCTV footage.

12.2 Individual access reports can also be provided to assist in disciplinary investigations and monitoring time and attendance etc. These requests will also be processed through the office of the security manager of a department, in terms of their internal protocols.

12.3 Please note that there is a high demand for individual access reports and these reports will be prioritised according to the date that it has been received and the client will be given an indication of when the report can be provided.

DIRECTOR: PROVINCIAL SECURITY PROVISIONING

DATE: 12/06/2016