agriculture &
rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF AGRICULTURE
& RURAL DEVELOPMENT
HEAD OF DEPARTMENT
Private Bag X 2039, Mmabatho, 2735
29 -10- 2024
RECEIVED
NORTH WEST PROVINCE
REPUBLIC OF SOUTH AFRICA

Organisation	**Department of Agriculture and Rural Development**
Programme	**Security Services**
Manual	**Security Procedure Manual Review**
Policy ref. number	**5/6**
Compiled by	**Security Services**
Approved by	
Date of effect	26/11/2024

INDEX

1. Introduction

Security procedure is a process in which security measures are applied to ensure that any object or a person that gains access to the department is safe, has a bona fide reason to enter, is entitled and authorized thereto, and the department and its employees will not be exposed to danger or a breach of security during his/ her presence on the premises.

This manual serves as a guide in ensuring superior value through delivering the right risk reduction strategies, solutions and services, and to provide leadership in the protection of official state assets and information against security risks and threats in the Department.

2. Purpose

This document provides a departmental framework for the implementation of the Minimum Information Security Standards and Minimum Physical Security Standards to monitor and control people and property. It will further ensure that departmental employees, visitors and service providers comply with the necessary security procedures to prevent or minimize security crime risks to the department. Security measures serve the interest of the people, and are therefore not meant to restrict or inhibit staff or visitors.

3. Objective

3.1. To promote uniformity in the execution of departmental access and assets control.

3.2. To provide a safe and secure working environment for employees, visitors and service providers.

3.3 To ensure that information is protected and access to information by the employees or external clients is properly controlled.

4. Scope

4.1. This Procedure Manual applies to the following individuals and entities:

- All employees of the Department of Agriculture and Rural Development.
- Contractors and consultants rendering service to the department, including their employees who may interact with the department.
- Interns and contract employees.
- Visitors and members of the public visiting the premises or officially interacting with the department.
- Intellectual property and Information.
- Fixed property that is owned or leased by department.
- All moveable assets, biological and natural (plants) assets that are owned or leased by the department.

5. LEGISLATIVE AND REGULATORY REQUIREMENTS

- Control of Access to Public Premises and Vehicle (Act 53 of 1985)
- Fire Arm control Act (Act 60 of 2000)
- Criminal Procedure Act (Act 51 of 1977)
- Trespass Act (Act 6 of 1959)
- Minimum Information Security Standards (MISS)
- Minimum Physical Security Standards (MPSS)
- Private Security Industry Regulatory Act (Act 56 of 2001)
- Public Finance Management Act 29 of 1999
- Public Service Act of 1994
- Constitution of the Republic of South Africa (Act 108 of 1996)
- Protection of Information Security Act 84 of 1982

- Promotion of Access to Information Act 2 of 2000
- National Archives of South Africa Act 43 1996
- General Intelligence Laws Amendment, Act No 11 of 2013
- Electronic Communication and Transaction Act 25 of 2002
- Protected Disclosure Act 26 of 2000
- North West Province Moveable Assets Policy and Procedure Manual
- Civil Protection Act 67 of 1977
- Fire Brigade Act 99 of 1987
- NWPG ICT Provincial IT Security Policy
- Departmental Security Management Policy
- Key Control Policy
- Records Management Policy
- National Key Point Act 102 of 1980
- Disaster Management Act 57 of 2002
- National Forest Act 84 of 1998
- Protection of Personal Information Act 4 of 2013

A. PHYSICAL SECURITY

6. ACCESS CONTROL

- Access control procedures are developed to minimize vulnerability and to reduce the threat or risks faced by the Department of Agriculture and Rural Development.

- The Control of Access to Public Premises and Vehicles Act, Act 53 of 1985, is applicable when entering and leaving the premises of the department.

- Verification of all visitors is necessary before access is granted; when a visitor arrives at the security reception area of the departmental premises, such a visitor shall identify himself/ herself positively.

- Identification includes the display of a RSA Identification document, passport or driver's license. In the case of SAPS/ SANDF/ SSA an appointment card must be displayed. Personal identification includes the identification of the visitor by a staff member. No other proof of identification is acceptable.
- The ideal situation is to reduce entrances/exits to the absolute minimum, to secure unnecessary access points, and to control those remaining.

- At each point at which access is to be controlled, Security Officers are responsible to manage and grant such permission. Turnstiles and locking mechanism, fitted with a means for activating it, is installed in or on the barrier. Access is then granted when the proper identification is made available either to the mechanism or Security Officer responsible.

- The private property brought in to the premises must be declared and be entered into the security registers so that on departure, no removal permit would be demanded by Security Officers at the time of removal, but the property would be confirmed in the Private Property Register, which is kept at Security Desk. **(Annexure 'F')**

6.1 **BIOMETRICS ACCESS CONTROL AND ACCESS CARDS: PERSONNEL**

6.1.1 With biometric reader access control, the Department can manage entry to its premises and movement between different areas and ensure security within its premises

6.1.2 Newly appointed staff members must be brought to the Sub-Directorate: Security Services for application of enrolment/application for access cards. Enrolment and access cards are issued on their starting date in the Department.

6.1.3 Newly appointees must bring along their ID books, letter of appointment with persal number.

6.1.4 Using own biometric/card to open for another person constitutes infringement of security procedure and such a security breach is regarded as misconduct in terms of Regulation 2 of Disciplinary Code and Procedure for Public Service as amended in 2003.

6.1.5 **If an employee is seen using his/her biometric/card to open for another person such card will be de-activated and the matter will be reported to the Director in charge for corrective actions.**

6.1.10 In case an official is struggling to have access even after being enrolled, this must be reported to Security Services immediately

6.1.11 Any loss of card has to be reported within 24 hours in writing to the Deputy Director: Security Services. In addition the person who loses the card under any circumstances may be required to report such loss at the nearest police, an affidavit or case number, depending on the nature of loss. Such particulars will be submitted to the Deputy Director: Security Services.

6.1.14 Upon termination of service for whatever reason i.e. suspension, transfer, and dismissal or in the event of death, the Director or delegate should:

- Immediately notify the Sub-Directorate: Security Services, in writing.
- Ascertain that the access card be collected and forwarded to the Sub-Directorate: Security Services and the official removed from biometric system
- In case of suspension, the biometric access/ card will be de-activated for the period of the suspension and an employee will be treated as a visitor

and access will only be allowed in consultation with the line function Director

Directorate: Human Resource Management should send list of all employees leaving the department, to the Sub-Directorate: Security Services at the beginning of every month.

6.1.15 A staff member who for any reason is not registered on the biometrics system or does not have his/her own access card will be treated as a visitor. **(6.2.2 below)**

6.1.16 Consultants and contractors who are going to work longer than two weeks in the department may be enrolled on the biometric system/ apply for access cards. Applications will be done through the hosting Directorates and **the Directorate that requests biometric access/ cards and keys for external service providers (Auditors, Contractors, etc.) is accountable for the safe return of such items**. If they are not returned at the completion of the project, **the Directorate will be responsible for replacement costs**

6.1 ACCESS: VISITORS

6.2.1 Apart from the control of employees entering and leaving the premises, all visitors must be controlled. Visitors include:-

- Contractors
- Consultants
- Other Government Employees
- Sales Representatives (**allowing sales representatives during working hours disrupts operations and service delivery as**

employees spend time listening to them than doing what they are employed for).

- Personnel family members

6.2.2 **Visitors cards:** All visitors, contractors, consultants and other service providers must be provided with the DARD visitor's access card

6.2.3 All access control cards must be returned to security at the end of each visit

6.2.2 **Visitors must be accompanied by a Security Officer or hosting employee on both entry and exit of the premises and must be restricted to the office visited.**

Measures to control visitors include:-

- Requiring visitors to report to the Security counter/ reception on their arrival.
- Confirming appointments, at the security desk, with staff prior to access being permitted to the premises
- The visitor will produce the identity document to the security officer and will sign the visitors register after his/her particulars has been entered by the security officer **(See Annexure B)**
- Fetching visitors from the security reception and escorting them back to Reception after the visit, by the host or the last employee visited.
- If a visitor does not have identity documentation, the person visited will vouch for such visitor by signing for the visitor in the register.
- If the staff member left his/her card at home his/her immediate supervisor will vouch for him/her.

6.2.3 Section 2 (2) of Access to Public Premises and Vehicles Act 58 of 1985 exempt the members of SAPS, SANDF and SSA from the strict requirements

of access control when they enter the building in execution of their duties. But they must produce proof of identity (appointment card) to the satisfaction of the authorized officer concerned.

6.2.4 All staff members must co-operate in controlling movement of strangers on the premises, either by reporting their presence or enquiring as to their purpose on the premises, and where no satisfactory account is given, the stranger must be reported to Security Services.

6.3 SEARCHES

6.3.1 Searches are regulated by means of the Control of Access to Public Premises and Vehicle Act, (Act No. 53 of 1985). All persons entering the premises shall be subjected to search. They shall also subject anything which he/she has in his/her 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. The objective is to prevent prohibited items from entering the premises and unauthorized assets from leaving the premises.

6.3.2 In case of physical inspection, every person shall open and show the contents of his/ her jackets, attaché case, handbags, shopping bags, or any other object. In case of technical aids persons and equipment will be subjected to searches by means of metal detector and or X-ray machine.

6.3.3 Every vehicle that enters or exits the department will be subject to random vehicle searches. The only exception will be emergency vehicles when responding to an emergency, the vehicle of the MEC and Accounting Officer.

6.3.4 Vehicle searches will include at a minimum the engine compartment, boot or cargo space, undercarriage, passenger compartment and wheel wells.

6.3.5 Pool vehicles will be recorded, kilometer readings at the start and end of the authorized trip, will be entered in the Vehicle Register.

6.4 PARKING WITHIN THE PREMISES

6.4.1 All officials authorized to park within the premises must comply with the security procedures of the premises i.e. searches when entering and leaving the premises.

6.4.2 All officials parking at the access controlled areas must be enrolled in the biometric access system for the purpose of accessing such parking

6.4.2 Where the private vehicles are parked inside the department premises or a car park that is provided by the department within the premises, such parking will be at the vehicle owners' risk. The department will not be liable for any damage, theft of or out of the vehicle.

6.4.3 Officials must ensure that their vehicles are parked only on the allocated parking bay, where applicable.

6.4.4 All irregularities identified with regard to the parking area must be reported to the Security Services immediately.

6.4.5 Unauthorized vehicles will not be permitted in the parking area if prior arrangements were not made with the security manager or any authorized official.

6.4.6 Officials are not allowed to give their parking bays to other persons for the periods while they are not utilizing their parking bays.

6.4.7 Vehicles may not be washed in the parking areas and the use of fire hoses for these purposes is considered as an offence. This must immediately be reported to the Security Manager.

6.4.8 Officials making use of Government vehicles may not use any other parking bays other than the allocated bay for that particular vehicle.

6.4.9 Officials who have parking in the building (underground parking) must ensure that no unauthorized persons gain access to the building. All visitors must enter the building via the main entrance of the building.

6.5 AFTER HOURS CONTROL

6.5.1 Control of access after normal business hours will include:-

- All employees returning or remaining in their offices after normal working hours must notify security at reception and they must be booked in and out in the After-Hour Register. **(See Annexure 'A')**

- The time of entry to, and exit from the premises after business hours of all persons will be recorded manually.

- The statistics of staff working during weekends and public holidays will be monitored in order to adjust the ratio of Security Officers to be able to patrol inside the two buildings effectively.

- Service providers or temporary/ casual staff will not be given access to the premises unless an arrangement is made with the Sub - Directorate: Security Services.

- All short term (i.e. day to day) contractors working in the buildings shall be escorted by the employee who arranged that such work should be done. The employee shall supervise and be responsible for the

movements of the service provider while in the buildings and report any irregularity/ security breach to the Sub-Directorate: Security Services.

- **The Security Services will from time to time conduct after hour inspection to ensure compliance to office security. This exercise might include law enforcement agencies such as SSA (State Security Agency) as they have a legal mandate to protect state property.**
- Such inspection will be conducted with the permission of Head of Department
- Visitors are not allowed into the premises after hours.
- No officials will be allowed to sleep (overnight) in or on the premises of the department
- The Security Officers will do after-hours inspection to check whether all the doors and windows are closed and locked.
- The Security Officers will randomly patrol the premises and any security or safety breach is noted, it will be reported immediately.

7. KEY CONTROL

7.1 The Sub-Directorate: Security Services is responsible for key control and record keeping of keys of all offices

7.2 Office allocation and maintenance is the responsibility of Directorate: Supply Chain Management. Allocation arrangement will then be communicated, in writing, to Sub – Directorate: Security Services for issuing of keys. **(Key application form, Annexure 'C')**

7.3 Specific individual from Security Services should be appointed in writing as a Key Custodian.

7.4 Any loss of key has to be reported within 24 hours in writing to the Deputy Director: Security Services. In addition the person who has lost key under any circumstances may be required to report such loss at the nearest police station. An affidavit or case number, depending on the nature of loss must be produced. Such particulars will be submitted to the Deputy Director: Security Services.

7.5 Depending on the circumstances of the loss the person who lost the key may be required to pay the replacement cost at Directorate: Finance and take the receipt to Security Services to apply for a new key.

7.6 Duplicate keys kept for emergency use must be sealed and stored in prescribed cabinets. Only Assistant Directors and Deputy Director: Security Services can give permission to break a seal.

7.7 All other duplicate keys must be kept at the appropriately secured place or inside the safe where only the appointed Assistant Key Control Officers/Key Custodian will have access.

7.8 When the key is left at home, a written motivation to open the office has to be given through the manager, to the Sub-Directorate: Security Services **as per Key Control Procedure 7.3**

7.9 No office will be opened without the knowledge of the occupant and/or the permission of the relevant Director/Delegate in writing. It should be noted that this arrangement will apply only for work related matters.

In all instances the items or information that is to be retrieved should be specified in the form. 'Annexure M'

7.10 The duplicate keys of registries and other sensitive areas have to be stored in a properly sealed envelope by Key Control Officer/Key Custodian with proper record keeping.

7.11 The Key Custodian has to ascertain that duplicate keys are available and safeguarded for every office.

7.12 The Key Control Officers will safeguard duplicate keys and the most recent lock combinations which must remain sealed in the envelopes in which it has been received.

7.13 When a need to open more offices is identified in any work that is to be carried out by either staff members or external i.e. Auditors, contractors etc., Security Services should be informed in writing at least three days before.

7.14 The office keys must be returned to the Key Control Officer by the official who is resigning or being transferred or for any reasons terminating his/her services to the Department. Where the circumstances are beyond control, for instances due to death, the supervisor must collect and submit the keys to Security Services.

7.15 In the case where the official is being transferred or for any reasons terminating his/ her services, the office key and the access card must be returned to the Key Custodian.

7.16 The duplicate keys kept for emergency use must be sealed and stored in prescribed cabinets. Only the Deputy Director: Security Services or his/ her delegate may give permission to break a seal

7.17 SAFE KEYS AND COMBINATIONS

7.17.1 Every user of a safe shall ensure that the combination and/ or duplicate keys are sealed in separate envelopes and kept by the key custodian with the following particulars displayed on the envelope:

- The date of sealing by affixing an official date stamp,
- Signature of member(s) sealing the envelope,
- The serial number of the relevant safe/ strong room and,
- The office number and location of the office in the building in which relevant safe/ strong room is situated

7.17.2 One safe key must be handed to the custodian

7.17.3 Only a person in direct control of a safe with the combination may set the combination

7.17.4 A previous safe combination may never be re-used.

7.17.5 The user of the safe shall ensure that the combination to a safe is changed under the following conditions

- Every three months
- If someone else takes over the control of the safe
- If any indication exists that the combination has been compromised
- If a new lock is installed

8. CONTRACTORS

8.1 All contractors and delivering companies will be subjected to the Access Control principles.

8.2 However if contractors are going to perform any duties inside the premises, the following procedure should be followed:

- A letter of confirmation from the responsible directorate indicating the reasons for entry, name, address and contact details of the contractor.

- Where applicable the contractor and employees will apply for the access control card through director/delegate and comply with the conditions of application and the use thereof.

- If the contractor brings in tools and equipment, a Tool/Equipment List which is obtainable from Reception will be completed and a copy thereof will be left with the Security personnel. Every time the contractor wishes to take out or in tools, they will be checked against the completed list and an update will be done accordingly. **'Annexure E'**
- If the contractor has to do any work in the offices of the senior management staff, such work will be performed under the supervision of the officials from the Security Services.

- Access and work in any other offices will be supervised by the occupant or the officials from Security Services in the absence of the occupants.

- In both cases a written notice should be submitted to Sub – Directorate: Security Services at least five days before commencement of the work.

- If the contractor needs to work after-hours, weekends or public holidays, the Security Services should be informed in writing through the responsible directorate, at least five days before commencement of the work.

9. OFFICE SECURITY

9.1 All staff members must be advised during induction that the department is not responsible for loss or damage in respect of their own personal property.

9.2 Staff members must not leave valuables unattended on desks and they must also lock away or remove personal property whenever practicable.

9.3 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 the Security Services immediately.

9.4 Cleaning of offices should only be done during official working hours, supervised by the occupant of the office. **Offices must be kept locked at all times when the occupant leaves the office, even for a short period of time.**

9.5 Cleaning of offices should be done preferably by in – house cleaning officials who have been vetted and in the presence of occupants.

9.6 Office keys must not be placed above the door, in pot plants, behind fire equipment etc. but be kept in the official's possession.

9.7 Office keys must not be left in the door locks as other persons may identify the key number and purchase a duplicate key to access such office.

9.8 The staff members must ensure that drafts of sensitive or classified documents are not left exposed on the table or thrown in the dust bins. The drafts which are not used anymore should be shredded.

9.9 At the end of the day, before departure, each member should, where applicable ascertain that:

- Lights and electrical appliances are switched off.
- Blinds and curtains are drawn.
- Doors/windows, safes and cabinets are closed/locked.

- Kitchen and ablution facilities water taps are closed

10. CONTROL OF ASSETS MOVEMENT

10.1 Acquisition of assets

- Contrary to any other proof, all moveable assets, including consumables become the property of the department upon entry onto the premises

10.2 Removal of the Departmental Property

10.2.1 The following procedures must be strictly adhered to in the event of removal of the Departmental property from the premises.

- The official must request permission in writing, to remove the assets.
- Authorization for the removal of property/assets permit must be completed fully. **'Annexure G'**
- Description of the equipment to be removed including the serial number and the asset identification number must be indicated in the permit
- Reason for the request must be stated in the permit
- Period for the requested permission.

10.2.2 The Director/Delegate must approve the authorization for the removal of property/Assets.

10.2.3 The permit must also be signed by the Asset Controller and Security Officer.

10.2.4 The original copy of the removal permit will be kept by the official authorized to remove the State property/Asset and the copy will be handed to security personnel who will compare the particulars with the property/assets and certify that it is correct.

10.2.5 The security personnel will keep the copy for record purposes and the official must keep the original copy as proof that he/she has the authority to have the property in his/her possession.

10.2.6 Official must take all the necessary steps to safeguard the property while in their possession and it must not be left unattended to in a vehicle.

10.2.7 Official is not allowed to remove the state property unless the security officer checks it. The security officer must append his/her signature on the original copy as a proof thereof.

10.2.8 Security Officers do not have the authority to give officials permission to remove goods from the building.

10.2.9 In the event of the property being stolen or lost it must be reported to the SAPS and to the Security Services within 24 hours. **'Annexure I'**

10.2.10 When the consumables and stationery have to be removed from the premises, designated form will be completed and be signed by the authorizing director/delegate. **'Annexure D'**

10.3 Private property brought on DARD Sites

- Private property brought onto the premises must be declared at the main security entrance point and a detailed description of the equipment must be entered into a security register for record purpose. A Private Property Register will be available for this purpose. **'Annexure F'**

- The contractors who bring equipment and tools will be required to complete a tool/equipment list upon entry into the premises. Such list will be completed in duplicate; one copy is retained by the security officer/designated person the contractor retains the other copy. **'Annexure E'.**

- When the contractor removes properties from the premises, such properties will be checked against the completed list. It is the responsibility of the contractor to update the list accordingly when the properties are removed or brought onto side.

10.4 Disposal of Assets

- If the asset disposal documentation is different from the removal permit such documents will be attached to the removal permit and all instances the assets should be fully described.

- The Security Services should be informed about disposal requests, the disposal methods, dates and venues.

- The Disposal Certificates and/or Assets Removal Permits should be produced to security officers before the assets could be removed from the premises for disposal.

- Before IT equipment could be disposed, they should be cleared of any information by IT technician and a report to this effect should be submitted to the Security Services

10.5 WASTE MANAGEMENT

- All the recyclable materials will be removed from the premises by an authorized Waste Management or Recycling Company only.

- Depending on the nature of the material, description documents, mass, should accompany the removal permit.
- In the absence of any agreement, a normal procedure with regard to Removal of Departmental Property (10.2) above will apply.

- **Transportation Compliance**

  The service provider must observe the following road transportation regulations National Road Traffic Act 93 of 1996 – R225; National road Traffic Regulations – Chapter 8 – Regulations for the identification, classification, packaging and transportation of Dangerous goods and Substances by Road as listed in SABS Code 0228, SABS 0229; SABS 0232-1 Emergency Information Systems Part 1 named Emergency Information Systems for Road Transportation[13]. Vehicles transporting dangerous goods listed in SABS 0228 must be fitted with the appropriate placards/decals as described in this code.

10.6 REPORTING OF STOLEN PROPERTY (PRIVATE AND STATE PROPERTY)

10.6.1 All security breaches, potential or suspected security breaches which include thefts; fraud; loss; etc. must immediately be reported to the Security Services and the relevant local SAPS

10.6.2 If theft/loss or damage to departmental property has occurred outside the premises of the department and it is impossible to report such loss/damage to the Security Services, the matter should be reported to the nearest police station and at the earliest opportunity, to Security Services. The matter should be reported within 24 hours.

10.6.3 If theft/loss or damage to departmental property has occurred inside the premises of the department, the matter should be reported to Security Services immediately and they will advise on further actions.

10.6.4 When reporting, full details surrounding the circumstances which led to a loss, with a full description of equipment, etc. which includes all parts and serial numbers, affidavits and case numbers, where applicable, should be provided. **The report must be in writing.**

10.6.5 The Deputy Director: Security Services may contact one of the following Security departments namely, SAPS, SSA (State Security Agency) or SANDF to assist with the investigation in the event of a security breach.

10.6.6 If the internal investigations reveal that the negligence on the part of the employee contributed to the loss/damage of the property, any relevant legislations/procedures may be applied to recover the cost of the loss from the employee concerned.

10.6.7 All security breaches reported to the Security Services will be reported to the Head of the Department and relevant security cluster departments.

10.6.8 Breaches of security must at all times be dealt with using the highest degree of confidentiality in order to protect the official(s) concerned and prevent him/ her (them) from being unnecessarily done an injustice to.

11 FIREARMS CONTROL

11.1. In terms of section 98 of the Firearms Control Act, (Act 60 of 2000), the Accounting Officer (HOD) must appoint a Firearms Control Officer for the managing and control of the firearms which are owned by the department.

11.2. In case of the firearms owned by the department, safe keeping, issuing and control of the firearms will be the responsibility of the appointed Firearm Control Officer.

11.3 All the state owned firearms and rounds shall be kept at a designated safe and if an authorized staff member need a firearm for execution of his/her duties, such firearm will be issued in terms of the provisions of the Firearm Control Act and it should be returned to the Firearm Control Officer within 24 hours after use.

11.4 No firearms will be allowed into the premises except those owned by the department.

11.5 In terms of Section 3 of the Control of Access to Public Premises and Vehicles Act, 1985 (Act No.53 of 1985), the members of South African Police Services, South African National Defense Force, State Security Agency and Correctional Services are exempted from this condition if they are in the premises to execute their duties.

11.6 Where applicable, the department will provide safes at the entrances of its premises. Visitors and employees who carry their private firearms will put such firearms into these dual lockable safes. One key will be kept by security officer, the other by the owner and the owner will complete and sign the Private Firearm Register. **'Annexure H'**

11.7 No firearms are allowed into the buildings in terms of the Firearms Control Act, 2000 (Act No.60 of 2000). Premises of the Department of Agriculture and Rural Development have been declared Gun free zones .

12 CONTINGENCY PLANNING

12.1 All emergencies must immediately be reported to Security Services and if possible to an OHS Reps

12.2 The Security Services in turn will liaise with the OHS Reps and the emergency will be reported to Emergency Services if it is necessary.

12.3 All Heads of Components/Directorates must ensure that all their subordinates are familiar with the Departmental Contingency plan.

12.4 All newly appointed personnel must be oriented on the direction of the emergency exits, the assembling points and be introduced to contingency officer on each floor.

12.5 All personnel must be informed of the Contingency Officer, Deputy Contingency Officer and other functionaries on their floors.

12.6 In case of emergency, officials must not panic and create alarm as this may lead to chaos and result in the loss of lives and injuries.

12.7 Staff members must obey instructions given by members of OHS Reps, Contingency Officers and functionaries on their floors.

12.8 All staff members must report at the assembly points indicated in case of an evacuation of the buildings.

12.9 The lifts must not be used during evacuation of the buildings.

12.10 The visitors and the physically challenged staff members must be assisted in case of an emergency.

12.11 Visitors need to be assisted by officials in the event of an emergency as the contingency plan is not known to them.

12.12 It should be noted that where the premises is equipped with public address (PA system), such system will be used for emergency purpose only, e.g. fire, bomb scare, floods, things that are health hazard, etc.

12.13 Procedures for evacuation of the facility in case of security threats or breaches of security

12.13.1Evacuations

A minimum of two (2) evacuation exercises should be performed during a twelve month period, according the Health and Safety Act. OHS Reps must perform these tasks.

12.13.2 In the event of an Emergency the following Procedure must be adopted

- Inform the Security Services, the OHS Reps and Security reception area
- Appointed Contingency officers in your area will take charge of the situation. They should be wearing high visibility vests
- Keep calm to avoid panic, confusion and injury
- Know the location of the nearest fire exit in your area
- If the building needs to be evacuated an announcement will be made
- Follow the directions of the Contingency Officers and evacuate the building
- Assemble on the pavement area in front of the building where it is marked Emergency Assembly Point
- It is the responsibility of all employees to prevent if possible, fire or any other crisis

12.13.3 Fire Equipment, escape routes and signage

- Fire equipment is only to be used during ~~an~~ fire emergency
- The building must be equipped with an electronic fire smoke detection and warning system
- Fire escapes are clearly marked and must be kept clear at all times
- All fire escapes are monitored and in case of emergency controlled by security officers.
- In order to comply with the OHS Act (Act 85 of 1993) fire drills will be held at the discretion of the OHS Unit
- Fire drills will be held in conjunction with the local Fire emergency services. In order to comply with the act the department should have at least two (2) fire drills per annum

12.13.4 First Aid and First Aid Room

- In order to comply with the provisions of the Health and Safety act certain employees must be trained in First Aid. They will provide First Aid during emergency situations.
- All injuries no matter how minor need to be reported to the OHS Unit
- A fully equipped First Aid Room should be situated on the ground floor. Employees in need of First Aid treatment can report at the security reception. The First Aid room should be available to all employees during normal working hours

13 NATIONAL FLAG

13.1 Instructions for display of the National Flag in the Republic of South Africa as announced in the Government Gazette (1774) of 9 August 1985, must be followed:

13.2 The National Flag must be displayed daily from 07:00 to sunset at the flag stations of Head Office, District Offices, Local Development Centers and any other institution of the department.

13.3 No flag other than the National Flag may be displayed without the prior, specific instructions of the office of HOD, through the Directorate: Communication

13.4 Flags of the following sizes must be used:

270cm X 180cm - for ceremonial use
180cm X 120cm - for general use
90cm X 60cm - for bad weather or for office use with a flag stand.

13.5 Should a flag in use become torn, it must be replaced.

13.6 Flag posts must be mounted either in front or on top of a building in order to make the flags as prominent as possible.

13.7 Flag posts must be erected and mounted in such a way that it could easily be removed for painting and repairs.

13.8 Wind indicators and decorations are not allowed on the flag posts

13.9 Flag posts for the national flag, must as far as possible be equipped to handle two sets of hoisting ropes to prevent any delays in the hoisting of the flag at the appropriate hour. When the national flag is displayed with another flag, the national flag is hoisted first and lowered last.

13.10 Apart from these days, the flag for ceremonial purposes may also be hoisted on special occasions, as instructed by the office of the Premier.

13.11 The flying of the national flag at half-mast as a sign of mourning must only be done on the instructions from the Office of HOD, through Directorate: Communication

13.12 Regular flags (180cm X 120cm) will be displayed daily during office hours. Storm flags (90cm X 60cm) may be used during bad weather.

13.13 When the national flag is flown vertically against a wall, the red band should be on the left-hand side of the spectator, and the rope seam at the top. When the flag is displayed horizontally, the seam should be on the left-hand side of the spectator with the red band at the top.

13.14 Except when specified otherwise, the Directorate: Communication Services is responsible for the hoisting and display of flags in the department.

13.15 All buildings occupied by State Departments are acknowledged as flag stations and therefore authorized to fly the national flag.

14. SECURITY COORDINATION AT DEPARTMENTAL EVENTS

14.1 With the identification of special events for the department that involves the office of the MEC of DARD, Minister and Deputy Ministers of the Department of Agriculture, Rural Development and Land Reform and any other related departments, the Deputy Director: Security Services must be informed in time of such events. The following security procedures will be addressed:

14.2 Liaison with the SAPS Provincial Director: Protection and Security Services and State Security Agency (SSA) where applicable for the purpose of TSCM or any other related pre-event exercise that will contribute to the safe hosting of the event.

14.3 Advice on the suitability of the venue, holding rooms, briefing sessions and escape routes.

14.4 Understand the orders of proceeding and have a draft program/program.

14.5 Liaise closely with the main organizer of the event and service providers.

14.6 Link with the following stakeholders:

- Traffic Department
- Local Police Station
- Emergency Management Services
- Fire Department
- State Security Agency (SSA)

14.7 Ensure that all service providers, through SCM, have been screened.

14.8 Ensure that a certificate of safety in terms of Disaster Management Act is issued for the safe utilization of stage, marquee, podium, tents etc.

14.9 Identify any marches or public gathering and ensure that an application for public gathering in terms of Public Gathering Act is made at the local office of the Department of Public Safety.

14.10 Ensure the appointment of a protocol officer.

14.11 Deploy security officials.

14.12 Secure and control parking areas.

14.13. Escorting of VIP members.

14.14 Contingency Planning.

14.15 The Security Services will after attending a briefing meeting with the law enforcement agencies, compile a Security Operational Plan for the event and a report after the event.

15. GENERAL SECURITY PROCEDURES

15.1 The Deputy Director: Security Services must be approached for advice or requests with regards to any physical security needs of all Departmental Directorates, to ensure that all the physical security measures are in accordance with the Departments total security plan and other acts and regulations applicable. This also includes the supply and installation of office locks and keys or any other security measure.

15.2 All defects to the security systems, doors, locks, etc. security risk, hazard or any other aspects which may result in the loss of lives or property or injuries must be reported to the Security Services within 24 hours.

15.3 All the security registers are classified as "Confidential' and should be in the custody of the Security Services, stored in secure lock up steel cabinets. Any other documents/records will be stored at registry.

15.4 If the copy of the register is required to be used as evidence in any matter, the request will be made in writing, through: Security Services. The security registers shall be used to investigate misconduct or intimidate employees.

16. CLOSED CIRCUIT TELEVISION (CCTV)

16.1 When installing CCTV system, several components will be taken into consideration, such as the following:

- Careful consideration on the position of the cameras
- Cameras are not hidden from view and are sited in such a way as to ensure that they only monitor spaces intended to be covered
- Signs are displayed so that everyone is aware that they are entering a premises that is covered by surveillance equipment
- Signs indicate the purposes for which cameras are installed

16.2 **The CCTV system procedures:**

- The main system is locked and stored at a secured area, controlled and managed by the Security Services
- Any request for footage must be done on the *CCTV Footage Disclosure Register*. Annexure O
- CCTV viewing by unauthorized or unqualified staff will be carried out in accordance with the relevant procedure ensuring that privacy and data protection is maintained
- CCTV can record personal data in the form of a person's face and may indicate 'special category' personal data, such as a person's ethnic origin or physical disability.
- This means that live or recorded images and monitor screens will not be viewed by any unauthorised third party without a lawful basis i.e. the person(s) that appear and are identifiable from the footage
- There will be no disclosure of recorded data to third parties without a lawful basis, however, it is acceptable for the Department to disclose images to

law enforcement agencies (SAPS, Traffic Law Enforcement or even SANDF) for the purpose of prevention and detection of crime

- CCTV footage will be kept for a maximum of 60 days, unless an incident has occurred on the departmental premises and the footage is to be kept for a purpose

agriculture & rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Annexure 'A'

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

AFTER-HOURS REGISTER: AGRICENTRE BUILDING

DATE: _____ **POST:** _____

Date	Time In	Initials & Surname	Company	Official Signature	Directorate	Time Out	Name of Security

Annexure 'B'1

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

DATE: _____ **ACCESS CONTROL REGISTER VISITORS** **NAME OF SITE:** _____

VISITOR'S CARD NUMBER	TIME IN	INITIALS & SURNAME	RESIDENTIAL ADDRESS	COMPANY	CONTACT NO.	PURPOSE OF VISIT	ANY DANGEROUS WEAPON e.g. (FIREARM) Y=YES N=NO	CAR REGISTRATION NUMBER	SIGNATURE VISITOR	SECURITY OFFICIAL SIGNATURE	TIME OUT

agriculture &
rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Annexure 'B'2

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

DATE: _____ **ACCESS CONTROL REGISTER STAFF ONLY** **NAME OF SITE:** _____

TIME IN	INITIALS & SURNAME	RESIDENTIAL ADDRESS	COMPANY	CONTACT NO.	PURPOSE OF VISIT	ANY DANGEROUS WEAPON e.g. (FIREARM) Y=YES N=NO	CAR REGISTRATION NUMBER	SIGNATURE EMPLOYEE	SECURITY OFFICIAL SIGNATURE

agriculture &
rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Annexure 'C'

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES
SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

KEY REGISTER

NAME OF KEY HOLDER: _____

OFFICE NUMBER: _____ KEY NUMBER: _____

Date of issue: _____

I have read and understood the key policy of the department and I will comply with the contents thereof.

The cost of the Abloy is R 150.00, big cylinder key is R70.00 and small cylinder key is R40.00. The key holder will be liable for replacement costs if the key is lost or damaged negligently

Signature: _____

Key issued by: Name: _____

Signature: _____

Date: _____

Key returned by: **Name:** _____

Signature: _____

Date: _____

Reason:

_____

_____

Annexure 'D'

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

SECURITY SERVICES

TO : SECURITY SERVICES

FROM :

SUBJECT : REMOVAL OF STATIONERY/CONSUMABLES FROM THE DEPARTMENTAL PREMISES

Authorization is granted to (name) _____ for the removal of the following stationery/consumables items from (premises): _____ to (premises): _____ reason for removal: _____

Description of Item	Serial No.	Quantity

DIRECTOR/DELEGATE: _____DATE: _____ SIGN:_____
SECURITY OFFICER: _____DATE: _____ SIGN: _____

Annexure 'E'

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 3840153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

SERVICE PROVIDERS' TOOL LIST

Name of Service Provider: _____

Date of Entry	Description of Item	Date Out

Name of Contractor: _____ Name of Sec off: _____

Signature: _____ Signature: _____

Annexure 'F'

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

PRIVATE PROPERTY BROUGHT ON SITE

Date in	Initials & Surname	Description of item	Serial number	Security – check in	Owner's Signature	Date out	Security – check out

agriculture &
rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Annexure 'G'

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES
SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

TO : SECURITY SERVICES

FROM : ASSET MANAGEMENT

DATE : _____

SUBJECT : **REMOVAL OF EQUIPMENT/ASSET FROM THE PREMISES**

Please allow _____ an employee of DARD/Service Provider from: _____ to remove the following listed equipment/assets with the following description from the Departmental Premises _____ for _____ official/repairs.

Asset Description/Make	Serial Number	Asset Number

_____ _____ _____
Head: Directorate Signature Date

_____ _____ _____
Signature Date
Asset Management

_____ _____ _____
Recipient (Name) Signature Date

_____ _____ _____
Security Officer Signature Date

agriculture &
rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

ANNEXURE 'H'

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

DEPARTMENT OF AGRICULTURE AND RURAL DEVELOPMENT
PRIVATE FIREARM REGISTER

Key No	Make of Firearm	Serial No	Caliber	Issued to:	Sign	Issued by:	Sign	Returned by:	Sign	Received by	sign	Date

B. INFORMATION SECURITY

The Department has valuable information that needs to be protected; therefore applicable security measures must be respected and adhered to. It is the responsibility of all Managers and staff members to ensure that where information is exempted from disclosure, security measures are applied in full, such measures shall include but not limited to proper classification of such information. The provisions of the **Minimum Information Security Standards** (MISS) approved by Cabinet on 04 December 1996 shall apply.

Information Security consists of the following:

- Personnel Security
- Document Security
- Communication Security
- Computer (ICT) Security

16. PERSONNEL SECURITY

16.1 Personnel Suitability Checks (PSC)

Please note that pre-employment security screening is a mere preliminary record check to verify the integrity and does not constitute a security clearance

Pre-employment screening is applicable to all job applicants or employees, for permanent and temporary posts. All advertisements should clearly stipulate that applicants will be subjected to personnel suitability checks

During the recruitment and selection process all short listed candidates will be subjected to PSC. These include **(i)** criminal record checks and credit checks; **(ii)** citizenship verification; **(iii)** Identity verification, **(iv)** Matric and **(iv)** highest qualifications/study verification. All candidates/employees must consent to this otherwise their candidature cannot be considered

Each result, in terms of the 5 different areas as indicated in paragraph 16 above, need to be scrutinized and evaluated. During this process various factors must be considered and amongst others the following:

- Level and duties of the post, working environment, job specifications, level of responsibility, level of autonomy, management, access to information, type of information (sensitive, top secret, highly confidential, political), intellectual property, access to assets, facilities, etc.
- Where he/she shall serve, to whom will he/she report to, the environment of the office, manager's designation, responsibility, scope of work, visibility, (Position occupied) and etc.
- Seriousness of offence, when it occurred, etc.

16.1.1 **Procedure for requesting PSC**

- Personnel suitability check – HRM (Human Resource Management) office has to write a request for personnel suitability checks of all the shortlisted candidates for any post to Security Services at least **seven (7) working days before the interview**.

In the letter the following should be stated:-

- Date of the interview
- Address where the interview will be conducted
- Description of the Post
- Initials and surname and ID number of the shortlisted candidates

No employment offer shall be made prior to the outcome of the pre-employment screening process. An appointment will only be effected once a positive security screening has been obtained. Appointments include promotions and transfers.

❖ **Company screening** – The background check is the process of establishing the reputation and trustworthiness of service providers/ private businesses and their

directors. This process also seeks to ensure that the service providers conform to the laws of the country.

SCM (Supply Chain Management) should submit letter to Security Services requesting security screening of all the shortlisted companies in every tender or close bid, the following should be inclusive:

- Valid Tax Clearance Certificate
- Certified ID copies of Directors and /or partners
- BBBEE Certificate
- Registration Certificate of the company/closed corporation
- SBD4
- Quotes Signed by Services Provider

- Security Services will forward the information to State Security Agency for investigation and security screening process, and communicate results to the HOD's office.

- **The request should be done after evaluation but before awarding, failure to submit, the responsible manager will have to account to State Security Agency in writing of not complying with the security directives.**

- **Please note** that the requirements for security companies are that site inspections have to be conducted by Bid Evaluation Committee (Security Services and SCM) prior to the awarding of the tender. This is done to determine the risks, compliance and to check the preparedness of the prospective service provider.
- **No person or a company should be awarded tender to render service to the Department without a pre- security screening.**

16.2 **Declaration of Confidentiality**

- A Declaration of Confidentiality is an oath that every official has to take, assuring the Department that she/he will protect the Departmental information and that she/he will not divulge it to anyone. The purpose of this is for the protection of Departmental information.

- Employees of private companies' e.g. private security company, who by the nature of service they provide, may have access to information, have to complete the Declaration of Confidentiality form and be signed by the Commissioner of Oath, and returned to Security Services on the same day. **'Annexure K'**
- All interns in the Department have to complete the Declaration of Confidentiality form.

- The Declaration of Confidentiality form is available at the Security Services offices.

16.3 **Security Vetting / Clearance**

- Security Vetting is the systematic process of investigation followed in determining a person's security competence.

- It is stipulated in the Minimum Information Security Standard (MISS) document that, from the lowest level up to the HOD, all staff members and any other persons who will have access to classified information must be subjected to security vetting.

- Security Vetting is part of a counter-intelligence system used to protect the sensitive information of the Department and other possible threats

- The main focus of the security vetting process is to determine the integrity, reliability and loyalty of an official towards the Republic of South Africa and its Constitution.

❖ All employees who have access to classified information should be subjected to vetting and the following forms should be collected from Security Services and be completed and returned to the same office within 31 days.

16.3.1 **Security Vetting forms:**

- Z204 (Security Clearance Form)
- Vetting Application Certificate (to be completed by the supervisor of the applicant).'**Annexure J'**
- Declaration of Confidentiality. **'Annexure K'**
- SAPS Fingerprint Form. 'Annexure L'
- Applicant/ Employer' Indemnity Form M'

16.3.2 **Documents (Page 2 of Z204 form) to be attached**

- Certified copy of ID and passport (if available) of applicant, spouse or partner
- Certified copy of marriage and/or divorce certificate
- Certified copy of academic qualifications
- Copy of latest salary advice
- Copies of all bank statements: savings, cheque, credit card(s), bond accounts and other financial loans. **These should cover the recent four months.**
- Declaration of directorship(s) in business venture(s)
- One passport size recent colour photo of the applicant

All applicants are advised to read the Z204 form before they complete.

❖ The Sub-Directorate Security Services is responsible to verify that the Z204 forms are correctly completed and all the requested documents are attached. All the completed Z204 forms will be handed to State Security Agency (SSA) to complete the process of vetting.

16.4 **Upgrading of Security Clearance**

- The upgrading of a security clearance is conducted when/ if an employee's got a higher post or got transfer to a different post were she/he will have access to classified information, she/he will be re-vetted.

16.5 **Levels of Security Clearance and the validation**

- Confidential - 10 years
- Secret - 5 years
- Top Secret - 5 years

- **Confidential** > this category is for employees who have access to information that can harm the objectives and functions of an individual and/or Department if such information is leaked to malicious/opposing/hostile element.

- **Secret** > this category is for employees who have access to sensitive/classified information that can result in disruption of the objective and functions of the Department if such information is leaked to malicious/opposing/hostile elements.

- **Top Secret** > this category is for employees who have access to sensitive/classified information that can result in the neutralization of the objectives and functions of the Department and/or state if such information is leaked to malicious/opposing/hostile elements.

  A security clearance gives access to classified information in accordance with the level of security clearance, subject to the need-to-know principle.

16.6 **Transferability of Clearance**

- A security clearance issued in respect of an Official while he/she is attached to the Department is not transferable to another department.

16.7 **Immigrants Without RSA Citizenship And Persons With Dual Citizenship**

The official must be in a possession of residential permit and work permit. Every case will be treated on its merit.

16.8 Officials Traveling Abroad

When officials are traveling abroad they must be on their guard against any attempt by a foreign intelligence service to recruit them. If a person is approached, he/she must, immediately on returning, report the information in writing to the HOD or Deputy Director: Security Services for reporting to State Security Agency. While travelling, officials should maintain a low profile and be careful not to place themselves in compromising situations.

For the purpose of safeguarding departmental staff against foreign intelligence, all staff that are intending to visit abroad either private or official should inform the Security Services before departure through completing the departmental travelling/visit abroad application form attached as **'Annexure N'**

16.9 Protection of Executive Officials

Since Executive Officials are constantly the target of enemies of the State, the necessary precautions should be taken to protect these officials against threats of blackmail or violence. Such threats should be reported to Security Services.

17. DOCUMENT SECURITY

17.1 Classification and Reclassification of Documents

- The Department has at its disposal intelligence/information that is to some extent sensitive in nature and requires security measures. The degree of sensitivity determines the level of protection, which implies that information must be graded or classified.

- Every document must be classified on its own merit (in accordance with its own contents), and in accordance with origin of its contents, and not in accordance

with its connection with, or reference to some other classified document. This is done provided that where the mere existence of a document referred to is in itself information that calls for a higher security classification than the document containing the reference, the latter document must be classified accordingly.

- Documents that need to be classified are the following:
  - Personnel files e.g. Legal files, EPMDS files, personal information etc.
  - Clients' information e.g. Business plans, personal information etc.
  - Tender documents
  - Clients' business profiles
  - Anti-Corruption files
  - Risk assessment files
  - Procurement Plans
  - Financial records e.g. Salary, etc.
  - Security Registers

- The above mentioned files should be classified as Confidential. It is not all of us who need to know the said information; it is only for the people who qualify according to his/her level of clearance he/she obtained, or qualify according to their job description. The need to know principle has to apply in this case.

- The author of a document or Security Services must guard against the under-classification, over-classification or unnecessary classification of documents.

- When a document is classified, the classification assigned to it must be indicated clearly on the document in the following manner:-

- The classification of loose and not permanently bound documents and bound volumes (letters, books, publications, pamphlets) and other documents that are securely and permanently bound is typed/printed or stamped at the top and the bottom (preferably in the middle) of every page (including the cover).

- Security classifications should be indicated on such copies, photographs, sketches etc, by means of rubber stamps. The exact position of the mark may vary, depending on the nature of the document, so that essential details are not obscured by the stamp. An effort must, however, be made to mark the document as clearly as possible, so that the **mark will immediately attract attention.**

- Tracing or blueprints should be marked in such a way that the security classification is visible on all copies. Where this is not possible, rubber stamps should be used to mark all the copies.

- Rolled or folded documents, apart from being marked as prescribed on the face, a document such as this should also be marked in such a way that the security classification will be clearly visible when the document is folded or rolled up.

- In the case of tape recordings, certain photographs and negatives, it is physically impossible to place clear classification marks on a document itself, the document should be placed in a suitable box, envelope or other container and, if necessary, sealed, and the nature and classification of the contents clearly marked on the outside of the container.

- A clear distinguishing mark, the significance of which is known to those who deal with the file concerned, should be placed on both the front and the back cover of Confidential/ Secret/ Top Secret files.

17.2 **Access to Classified Information**

The general rules and prescriptions as to who may have access to or inspect classified matters are as follows:-

Persons who have appropriate security clearance or who are by way of their job description, with due regard being covered by the need-to-know principle.

- Persons who must necessarily have access to that classified information in the execution of their duties (the need-to-know principle) on condition that a suitable clearance has been issued or authorization has been granted.

- Personnel in posts such as stand-in typists/secretaries and other personnel in Components, who in general do not have access to classified material and who do not have a relevant security clearance, but are expected to have access to this information on an ad-hoc basis, on condition that the prescribed Declaration of Confidentiality must be completed.

- Persons who must necessarily have access to personal files or information that is in the personal file in the execution of their duties (the need-to-know principle) on

- Condition that a suitable clearance has been issued or authorization has been granted.

- Only authorized persons (e.g. Managers, Auditors, etc.) may be allowed access to classified files (e.g. Personal files of their subordinate), this is subject to the need to know principle.

- Managers are not allowed to take a member's personal file as it is, he/she can only access the information that he/she needs, and must ensure that it is handled with safe. No personal file or any confidential information must be left or be exposed to unauthorized personnel in anyway. Any information that is taken out of the member's file must be recorded in the register; it must also indicate when it has been returned.

- The personal file must not leave the Registry unless otherwise, the information needed from the file should be accessed at the registry. If it is physically taken out of the registry it should be registered in the relevant register, and be returned same day before knock- off time. It should be indicated in the register when it is returned.

- Classified information may be declassified for the purpose of availing it to the requester on the basis of Promotion of Access to Information Act (PAIA) and only after such declassification has been authorized by the Deputy Information Officer or designated person.

17.3 **Storage of classified documents**

- Classified documents that are not in immediate use must be locked away in an appropriate steel cabinet, safe or strong room.

- The doors of all offices in which classified documents are kept must at least be fitted with security locks, and kept locked when vacated, even if it is for a short period, whether a restricted area or not.

- To ensure a proper control over access to and effective control over movement within any place in which classified information is handled, an access control register must be kept up to date.

- Record of all classified and unclassified documents that are dispatched, distributed or made available must be kept to ensure proper control.

- Documents should not be left lying on the desk when the occupant leaves his/her office or work station and especially where classified information is being handled to minimize the possibility of a security breach.

- Strict access control should be implemented to registries where classified documents are kept.

- When classified documents are not in use, they must be stored in the following manner :

  - **Confidential - Reinforced filing cabinet**
  - **Secret - Strong room or Reinforced cabinet**
  - **Top Secret - Strong room or Walk-in-Safe**

- ❖ The keys to any place, room, strong room, safe, cabinet or any other place where classified material is kept must be looked after with utmost care and effective key control must be instituted. The keeping of the necessary key registers and the safe custody of duplicate keys and control over such keys must be strictly adhered to. The Security Services must be consulted for assistance in this regard.

17.4 **Loss of classified information**

- ❖ Should classified documents be lost or misplaced, this must immediately be reported in writing to the Security Services. An internal investigation in consultation with the HOD or his/her delegate whose Directorate the incident occurred must be instituted and appropriate, corrective steps taken. Such corrective steps must include but not limited to:-
  - Measures to prevent any recurrence of the incident;
  - Implementing measures that can support efforts instituted to minimise any negative impact that compromising of that particular information could have on the activities of the corporation;
  - Informing the parties concerned, that is, those divisions affected by the loss or potential loss of the classified information; and
  - Disciplinary steps against the person(s) responsible for the loss, if deemed necessary

17.5 **Registries and Files**

- ❖ Central Registries for Receiving of Incoming and Dispatching of Outgoing mail
  - An effective Registry is the core of effective control of document security. One Central/Main Registry in the Department must be where all incoming mail is received, opened and from where it should be distributed internally. The receiving and distribution must be recorded in the relevant registers.

- Outgoing mail must be forwarded to the central/main registry from where it will be dispatched, and it must be subjected to control measures and be recorded.
- Security seals should be used to dispatch personal files, classified mails and documents within the department and other organizations, record must be kept

❖ Access to Registries

- Access to registries should be controlled. No unauthorized person (any person that has no direct line functional responsibility inside the Registry) must be allowed inside registry.

- No file must be allowed to remain outside the registry for more than one working day. All files must be returned before closure on the same working day. Exceptions can be allowed, provided that storage facilities in the relevant office are on standard (as prescribed) and that the return of the file is followed up on a daily basis by the Head of the Registry

17.6 Removal of Classified Documents from Premises

❖ Removal of classified documents from the premises must be avoided, unless otherwise authorized by the HOD or his/her delegate for emergency and essential meetings outside the premises.

❖ All classified documents removed from the premises shall be recorded in the prescribed register.

17.7 Typing of Classified Information

❖ Classified documents may be typed only by persons having appropriate security clearance or authority from the HOD. Such typing must be done in a manner that will ensure that the information is not divulged to unauthorized persons.

❖ Drafts and copies of classified documents must at all times be treated as such.

17.8 Making Photocopies of Classified Documents

- All mechanical/electronic reproduction appliances should be properly controlled to prevent unauthorized or uncontrolled copying of classified documents. A Central/Main Photocopy Room is recommended to ensure proper control.

- Copies of classified documents should only be made with the approval of the authorized official appointed by the HOD or his/her delegate.

- Record of all duplicated classified documents should be locked away in a safe storage place.

17.9 Destruction of Classified Documents

- The National Archives of South Africa Act, Act 43 of 1996 applies to the destruction of classified documents.

- All draft notes, used carbon papers, ribbons, etc. of classified information identified for destruction should not be placed in waste-paper bins, but should immediately be destroyed or safeguarded until it can be destroyed as prescribed for the destruction of classified documents.

18. COMMUNICATION SECURITY

- To ensure a safe environment in which information of a classified nature could be communicated (electronically or verbally), the following guidelines must be followed:

18.1 Personal Communications

- Personal communication of a sensitive or classified nature must necessarily be subjected to strict self-discipline on the part of the communicator. In this regard the following guidelines apply:

- The need-to-know principle should be observed
- Such conversations should take place in such a way that sensitive information does not come into the possession of unauthorised persons or persons who happen to overhear what is said

18.2 **Telephone Systems and Facsimile Transmissions**

No classified information should be discussed on ordinary telephones, cordless or cellular telephones unless approved by the Provincial Government and encryption devices are used. No messages should be left on answering machines or voicemail systems which constitute a risk to information security. Classified information shall only be transmitted by facsimile when approved encryption devices are installed on the network.

18.3 **Offices used for discussing Classified Matters**

❖ Places such as offices, conference rooms etc., where sensitive or classified matters are discussed regularly, should be subjected to:

- Proper and effective access control.
- Regular Technical Surveillance Counter Measures (TSCM) (sweeping) by State Security Agency.

18.4 **Presence of Cellular Phones during Meetings**

For the fact that cellular phones are fitted with microphones and transmission capability, which may be exploited to unauthorised transmission of classified information, the chairperson of a meeting where classified matters are discussed, may use his/her discretion to ensure that there are no cellular phones in the conference/board room, office, etc., where such meetings are held. This is regardless of whether the cellular phone is switched on or off.

19. COMPUTER SECURITY

19.1 Security of Data Transmissions

Classified data transmissions should be protected by not exchanging password, be it computer or email, to ensure confidentiality.

19.2 Laptop and other mobile equipment

- The equipment belongs to the Department and not to any employee. Equipment is assigned to an employee in a particular post and it is his/her responsibility until he/she resigns or transfer to another post, etc.

- Employees that have been allocated laptops, digital cameras or any other mobile devices must take the utmost care in preventing theft, damage or loss of the equipment, this is to protect information.

- The basic rule for protecting a laptop is to treat it like a wallet or purse. It is advisable to keep a laptop out of sight when not in use, preferable in a lockable drawer or cabinet. **Do not leave your laptop on the desk in the office overnight.**

- Never let your laptop out of your sight in an airport or other public area. **Do not leave it unattended** at your seat or in the overhead storage. If you must leave it in a car, lock it in the boot out of sight. Avoid leaving your computer in a hotel room, if you must do so, at least keep it out of sight by locking it in another piece of luggage.

- In the unfortunate instance where any equipment has been stolen or lost, the responsible employee must report the matter to the South African Police Services (SAPS) within 24 hours. The case number and a detailed incident report must be submitted to Security Services and Asset Management in writing within 24hours

where applicable. The Security Services must conduct internal investigation and report to State Security Agency (SSA) in writing.

- **If it was the negligence of an employee, he/she must be liable for the payment of the equipment.**

19.3 **Passwords**

- All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be inserted into email messages or other forms of electronic communication, to prevent being accessed by unauthorized persons

NOTE: Do not share your passwords with anyone, including managers, administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Departmental information

- No one is allowed to gain access into one's computer without that person's authority, if the owner cannot be traced, then the authority must be granted by the Director in writing to the Security Services and Directorate: ICT, stating list of document/s or information needed. This will only be if there is any urgent need and proof of urgency, and in the presence of Security Services personnel.

19.4 **Internet Connections**

- The fire wall concept, that is, stand-alone computers with modems, or linked to any other system with appropriate firewalling, should apply to all Internet connections. Applications shall be subject to approval by the Provincial ICT.
- Employees are strongly discouraged to use any free Wi- Fi as it commonly used by hackers to infiltrate the laptops or cell phones.

19.5 **Intranet Connections**

- Intranet connections shall be subject to the same security measures as those applied in the ICT environment. Contractors needing access to the Intranet shall obtain such access only after approval by the Provincial ICT and be subject to this Security Procedure, directives and procedures regulating the use of Provincial Government's Intranet. No classified information shall be communicated over the Intranet unless protected by the approved cryptographic devices.

19.6 **Electronic Mail (E-MAIL)**

Classified information shall not be transmitted via e-mail unless authorised by the particular HOD or his/her delegate. Only communication systems equipped with the approved encryption devices may be used for transmitting classified information

20 Security breaches reporting

20.1 A Security breach is defined as the negligent or intentional transgression of or failure to comply with the prescribed security measures

20.2 Employees are expected to report incidents of crime in the Department (e.g. theft of documents, keys, access cards etc.)

20.3 A security incident includes:

- Evidence of tampering with information or systems
- Unauthorized access or repeated attempts of access to building or systems
- Theft or damages to state/private properties
- Social engineering incidents
- Loss/Compromise of sensitive information (Leakage)
- Damage to Systems/ Assets
- Financial Loss
- Injury to personnel, e.g. if there was a fight/robbery within the premises

20.4 Any employee who becomes aware of any deficiencies, losses or damages, whether caused by his /her improper application of security measures or not, must within 24 hours, report to SAPS and in writing to Security Services

20.5 All losses or damage to State property must be reported to the relevant line Director/Supervisor within twenty-four (24) hours

20.6 When security breach has occurred within the department premises, staff members are expected to report to the Security Services immediately and communicate the basic information according to the requirements of a report form: **Annexure I'**. Additional information might be requested during formal internal investigation (Statement)

20.7 When a security breach has occurred outside the department premises and it affects the department, employees must report the incident to the SAPS within (24) twenty four hours. The incident together with the case number must be reported to Security Services through the Manager of the concerned component as soon as possible.

20.8 Complete Report: the Security Services shall as soon as the investigation is complete, but within forty-eight (48) hours after the incident, submit a written report to the HOD

21. Security breach Investigation Procedure

- After receiving the incident report the ~~Deputy Director~~: Security Services will within three days share the report with relevant Directorates
- From the evidence gathered decision will be taken by Security Services to report the matter to SAPS and SSA, or formal investigation to be conducted
- The Security Services shall conduct an internal investigation to determine the circumstances that led to the security breach and advice the official accordingly. Should such an official still not observe the security measures even after receiving advice, the incident will be referred to the immediate supervisor of the official to take corrective disciplinary measures
- Thereafter, an investigation report indicating findings and recommendations will be submitted to the relevant Senior Managers

ANNEXURE I

AgriCentre Building
Cnr. Dr. James Moroka
& Stadium Rd
Private Bag X2039,
Mmabatho 2735
Republic of South Africa

CHIEF DIRECTORATE: CORPORATE SERVICES

SUB DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

Security breach report questionnaire

1. Name of Office/place where incident happened .....
2. Directorate.....
3. Sub Directorate.....
4. Name and Rank of Official Reporting.....
5. Contact numbers of the Reporting Official.....
6. Date and Time of Incident.....
7. What happened .....
8. How it happened.....
9. Who was responsible .....
10. What procedures and techniques were used by those responsible.....
11. What weapons and equipment were used.....
12. What damage was done.....
13. What was done about the incident.....
14. How effective were the existing security measures.....
15. How did the security personnel react to the incident.....
16. Any other aspects.....
17. What lessons can be learnt from the incident.....
18. Any recommendations.....

ANNEXURE J

VETTING APPLICATION CERTIFICATE

I, _____, hereby certify

(full names of the supervisor)

that _____ ID number _____

(full names of the applicant)

*His / her daily duties entail (post description):

_____

_____

_____

_____

_____

_____

The abovementioned duties allow *him / her access to the following classified / sensitive information:

_____

_____

_____

_____

Other fact / information that might influence this application:

_____

_____

_____

This application merits a security clearance to the level of: **Confidential/ Secret/Top Secret**

Signed at _____ on the _____ day of _____ 201__

_____ _____

(Signature) (Date)

ANNEXURE K

Declaration of Confidentiality

I, the undersigned _____

(Full names & Surnames)

I do hereby make oath and say:-

1.

I am an adult (gender) _____, employed by the Department of Agriculture and Rural Development (Component) _____ with Persal No._____.

2.

The facts stated in this affidavit are within my knowledge both true and correct.

3.

I have read Provisions of the Protection of Information Act, (Act 84 of 1982), specifically section 4 thereof.

4.

_____

Deponent

I certify that the Deponent has acknowledged that he/she knows and understands the contents of this affidavit, has no objection to the taking of the prescribed oath and considers the contents of the affidavit as binding on his/ her conscience. Signed and sworn before me at _____ on this the _____ day of _____ 201___, under my compliance with regulations contained in Government Notice No. R1258 dated 21 July 1972.

Commissioner of Oaths

NAME : _____

DESIGNATION : _____

ADDRESS : _____

APPLICANT/EMPLOYER' INDEMNITY

(FULL NAMES AND SURNAME)

: _____

ID No : _____

Residential Address : _____

TELEPHONE / CELL NO : _____

Have applied to be employed by / at prison employer by, (DEPT). ___, _____

In the capacity of : _____

I hereby authorize the above employer/the employer's duly authorized agent, namely to take / have

my fingerprints, together with my name, surname and identity number taken and make it available to the South African Police Service (SAPS). I furthermore authorize the South African Police Service (SAPS) to furnish personal information regarding my criminal background, criminal history, previous Convictions and/ or other relevant information such as is usually furnished by the Criminal Record Centre of the South African Police Service (SAPS) in this regard, to the above employer and/or the employer's duly authorized agent. I furthermore unconditionally indemnify the South African Police Service and all its members' employees as well as the Government of the Republic of South Africa against any liability which may result from furnishing information in this regard.

I understand that it is a condition of South African Police Service, that:-

(a) The information is furnished solely for the purpose of my proposed employment/ continuation of my employment with the above employer,
(b) Any information furnished to the employer/ the employer's duly authorized agent will be disclosed to me for comments before a decision is made on my employment/ application
(c) The employer/ employer's duly authorized agent is responsible for verifying the accuracy in every respect of the information furnished by the South African Police Service (SAPS).

Signed at: _____ On this (day – month- year) 20 - -

_____ _____

SIGNATURE OF OFFICIAL SIGNATURE OF APPLICANT

Pb/forms/Idemnity

agriculture &
rural development
Department:
Agriculture and Rural Development
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

AgriCentre Building Cnr. Dr. James
Moroka and Stadium Rd
Private Bag X2039,
Mmabatho
2735

CHIEF DIRECTORATE: CORPORATE SERVICES
SUB-DIRECTORATE: SECURITY SERVICES

Tel: +27 (18) 384 0153
Fax: +27(18) 384 4571
E-mail:MMaboya@nwpg.gov.za

ANNEXURE O

CCTV FOOTAGE DISCLOSURE REGISTER: AGRICENTRE BUILDING

Full Names of requester	
Directorate	
Date of request	

Details of Incident:

_____
_____
_____

_____
Signature

Request hereby Approved/ Approved with amendments/ not Approved

_____
_____
_____

_____ _____
Mr M. Maboya **Date**
Deputy Director: Security Services

REVIEW OUTCOME

_____
_____

Results/Conclusion

_____
_____
_____

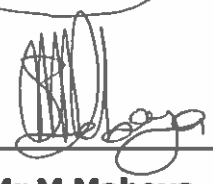
Name of Controller: _____ **Sign**_____ **Date:** _____

It is the responsibility of every employee of the Department of Agriculture and Rural Development to ensure that security measures and information security requirements are complied with.

Procedure Manual Review

This Security Procedure Manual shall be reviewed on an 36 months basis to keep it in par with the changes in the security environment and will be implemented after the approval.

Recommended/ not recommended

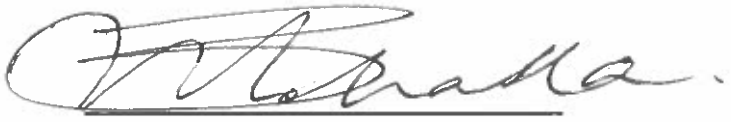


Mr M Maboya

Deputy Director: Security Services

Date: 2024/10/29

Approved/ not approved



Mr T.Z Mokhatla

Head of Department: DARD

Date: 25/11/2024