DEPARTMENT OF AGRICULTURE AND RURAL DEVELOPMENT

KEY CONTROL POLICY

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The main objective of designing the key control system is not only to deter unauthorized entry, but also to permit authorized entry to a large number of individuals or frequently changing staff. Information, personnel and property are critical important assets of government. The most important asset in our department will most certainly be our personnel, but without "information", which is seen as the foundation of the department, we would not exist or function successfully to meet our envisaged objectives.

1.2 Therefore, the information of the department is a target and we need to do all in our power to safeguard and secure the "information" in our possession. The steps to safeguard our assets may to a certain extent be seen as infringing our society's rights of freedom, but as we all have a joint responsibility in the safeguarding of our assets it is our benefit that we all adhere to the security rules and procedures laid down in our security policy.

2. POLICY STATEMENT

2.1 The Sub-Directorate: Security Services: Operational Security Services Unit is responsible for record keeping of keys of all offices.

2.2 The Unit is responsible for the key control of safes and vaults as well as combination codes of safes/ vaults

2.3 Deputy Director: Security Services as Key Control Officer should appoint specific individual in writing to be a Key Custodian.

2.4 Any loss of keys should be reported immediately in writing to the Sub-Directorate: Security Services after which the Unit responsible for access control would be informed to deal with the matter in terms of the Security Policy and Policy Procedure Manual

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

2.6 All other duplicate keys must be kept at the office where the appointed Key Custodian will have access.

2.7 In case a duplicate key is needed a written request and motivation counter signed by the Manager: should be forwarded to the Security Services. This will also be the case when the member left the keys at home or is not in office for any other reason and colleagues need to gain access into the office.

2.8 The duplicate keys of registries and other sensitive areas have to be stored in a properly sealed envelope (with its details on the outside) by Key Custodian.

2.9 The Key Custodian will safeguard duplicate keys and the most recent lock combinations, which must always remain sealed in the envelopes in which it has been received.

3. RESPONSIBILITIES OF THE KEY CUSTODIAN

3.1 Establish Key Control Register

3.2 The keys to the office must be strictly controlled.

3.3 The key custodian will only be the only person authorized to do the duplication of keys.

3.4 No person is allowed to have the master key or duplicate keys of the offices except the key custodian.

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

3.6. Duplicate keys kept for emergency purpose must be sealed and stored in the prescribed cabinet, only security management or the higher line functional managers can give permission to break a seal.

3.7. If a duplicate key is needed to open a particular office, a written motivation counter signed by the supervisor should be forwarded to the Security Services. This will apply even when an official left his/ her office key at home.

3.8. The duplicate keys of registries and other sensitive areas have to be stored in a properly sealed envelope by the key custodian to ensure proper record keeping. Sealed envelopes are subjected to controlling actions by the information security unit while the office head can implement measures to his/ her satisfactory.

3.9. Information regarding all security keys shall be entered in a record

3.10. Officials must adhere to the security measures as indicated in the key control policy and procedures.

4. OFFICE SECURITY

4.1. Each member is responsible to inspect his/ her own office or area of work for signs of intrusion at the beginning of each working day. If the member notices intrusions he/ she should immediately notify the head of the component or next senior member so that the matter can be reported to Security Services immediately.

4.2. Never leave the keys on the door; it must be in the possession of the person responsible for the office. This will prevent unauthorized persons from obtaining the keys.

4.3. The keys to filling cabinets, safes, etc. should only handled by the user. This key must never be left lying around or handled other persons.

4.4 Cleaning of offices should only be done during official working hours supervised by the occupant of the office of his/ her delegate.

4.5. The occupants must lock their office doors when leaving the office even in short intervals or during lunchtime.

4.6. The office keys should never be given to cleaning personnel. The occupant of the office is responsible for all activities taking place in their offices.

5. CAUSES OF WEAK KEY CONTROL

5.1 Insufficient record keeping system
5.2 Bad oversight
5.3 Irresponsibility by the user or person responsible for the keys
5.4 Lack of knowledge regarding the dangers of weak key control
5.5 An underestimation of the value of security
5.6 Weak or insufficient application of personal/ personnel security
5.7 Laziness on part of the user
5.8 The believe, by the personnel that there is nothing of value in this office, or nothing will happen
5.9 Then failure to adhere to security measures.

6.1 DANGER OF WEAK KEY CONTROL

6.1.1 Unauthorized personnel can gain access to the content of documents
6.1.2 Theft of documents, or other items
6.1.3 The photographic of the content of documents.
6.1.4 The placing of explosive devises.
6.1.5 The placing of eavesdropping devises in the office, or in the telephones and intercom systems
6.1.6 Arson
6.1.7 The committing of acts of sabotage.

6.1.8 Tampering with content of documentation or registers, such as fraud.

6.1.9 Compromising the confidentiality of information.

6.2 AT THE END OF THE DAY BEFORE DEPARTURE EACH OFFICIAL SHOULD ASCERTAIN THAT:

6.2.1 All electrical appliances are switched off

6.2.2 Blinds, curtains are closed

6.2.3 Doors, windows and cabinets are closed/ locked

7. KEY CONTROL PROCEDURES

The following Key Control Procedure must be adhered to:

7.1 NEWLY APPOINTED PERSONNEL

7.1.1 A person will report to Sub-Directorate: Security Services (MISS) and be issued with access card and sign for a key in a register.

7.2. LOST KEYS

7.2.1 Report to the Sub – Directorate: Security Services; they will advice on action to take.

7.2.2 Open a case or make an affidavit at the South African Police Service.

7.2.3 Written motivation has to be supplied with a case number (CR Number or Affidavit from SAPS) to the Sub - Directorate: Security Services through his/her supervisor.

7.2.4 The matter will be investigated and new key will be issued.

7.2.5 Employees will be responsible for the replacement costs of their

Lost their keys if the investigation find that the loss is due to negligence.

7.3. WHEN A PERSON LEFT HIS/HER KEY AT HOME

7.3.1 Written motivation has to be supplied through his supervisor/ or manager to Sub-Directorate: Security Services.

7.3.2 The key custodian will open the office for his/her and at the end of the day the key custodian will be notified to lock the office and sign the register. (NB. The office must be locked at all times when it is not occupied)

7.3.3 Employees are discouraged from leaving their keys at home.

7.4 WHEN A PERSON IS ON LEAVE/ SICK

7.4.1 When a person is on leave for more than five days, the keys must be sealed in an envelope and submitted to the key custodian per signature.

7.4.2 On arrival from sick/ leave a member reports to key custodian and sign for the key.

7.5 WHEN A PERSON RESIGN OR IS TRANSFERRED

7.5.1 In the case where an official resign or is being transferred or for any reason terminating his/her services, the office keys must be handed/ returned to the key custodian.

7.5.2 Where the circumstances are beyond control, for instance due to death, the supervisor should collect the key as well as the access card from the family and submit it to the Sub-Directorate: Security Services.

8. SAFE KEYS AND COMBINATIONS

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

8.1.1 The date of sealing by affixing an official date stamp.

8.1.2 Signature of member(s) sealing the envelope.

8.1.3 The serial number of the relevant safe/ strong room

8.1.4 The officer number and location of the office in the building in which relevant safe/ strong room is situated.

8.2

8.2.1 One safe key must be handed to the key custodian.

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

8.2.3 A previous safe combination must never be re-used.

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

8.2.4.1 Every Six months

8.2.4.2 If someone takes over the control of the safe

8.2.4.3 If any indication exists that the combination has been compromised.

8.2.4.4 If a new lock is installed.

9. LOSS OF COMBINATION / SAFE KEYS

9.1 Where the reason for the loss of a key is not known, the investigation shall be conducted.

9.2 In case of safe key combination is lost, the relevant programme shall arrange for a safe/ strong room to be opened by the contractor at the programme's own cost.

10. CONCLUSION

The establishment and maintenance of a condition of security is vital to the maintenance of the Department of Agriculture, Conservation and Environment's operational capability. It is the joint responsibility of all officials of the Department of Agriculture, Conservation and Environment to ensure that the minimum standards described in this policy are enthusiastically and thoroughly applied.

11. APPROVAL AND IMPLEMENTATION

This policy shall be reviewed after three years to make sure that it is in keeping with the changing environment and needs and will be implemented as soon as it is approved.

MS. O. BODIGELO-NYEZI

ACTING HEAD OF DEPARTMENT

DATE: 18/03/2026