



dpwr

Department:
Public Works and Roads
North West Provincial Government
Republic of South Africa

KEY CONTROL POLICY

PURPOSE

1.1 REGULATORY FRAMEWORK

- 1.1.1 The PFMA;
- 1.1.2 Basic Conditions of Employment Act.

1.2 SITUATION ANALYSIS

The establishment and maintenance of a condition of security is vital to the maintenance of the Department of Public Works and Roads operational capability. It is the joint responsibility of all Officials of the Department of Public Works and Roads to ensure that the minimum standards described in this policy are enthusiastically and thoroughly applied.

1.3 DESCRIPTION

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 Employee's rights of freedom, but as we all have a joint responsibility in the safeguarding of our assets, it is to our benefit that we all adhere to the security rules and procedures laid down in our Security Policy.

1.4 WHAT IT SEEKS TO ADDRESS

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 the frequently changing workforce. 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.

1.5 LINKS TO OTHER POLICIES

Occupational Health and Safety and Security Management Policies.

1.6 WHO WILL USE IT

This policy will be applicable to all DPWR Officials.

2. BENEFITS

2.1 HOW IT WILL REDUCE RISK

- 2.1.1 Unauthorized personnel cannot gain access to the content of Departmental documents;
- 2.1.2 Theft of documents or other items curtailed;
- 2.1.3 Photography of the content of documents curtailed;
- 2.1.4 Placing of explosive devises curtailed;
- 2.1.5 Placing of eavesdropping devises in the office, or in the telephones and intercom systems curtailed;
- 2.1.6 Arson;
- 2.1.7 Committing of acts of sabotage curtailed;
- 2.1.8 Tampering with content of documentation or registers, such as fraud, curtailed;
- 2.1.9 Compromising the confidentiality of information curtailed.

3. IMPLICATIONS OR INTENDED/ UNINTENDED CONSEQUENCES

None

4. POLICY

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

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

- 4.2 Deputy Director - Operations as Key Control Officer, shall appoint a specific individual in writing to be a Key Custodian. Only Security Officers who are employed by the Department will be appointed;
- 4.3 Any loss of keys should be reported immediately in writing to the Directorate Security Services after which the component/unit responsible for access control would be informed to deal with the matter in terms of the Security Policy;
- 4.4 Duplicate keys kept for emergency use must be sealed and stored in prescribed cabinets. Only the Director Security Services or his / her delegate can give permission to break a seal;
- 4.5 All other duplicate keys must be kept at the office where the appointed Key Custodian will have access;
- 4.6 In case a duplicate key is needed, a written request and motivation, counter signed by the Manager, shall be forwarded to the Security Services. This will also be the case when the member left the keys at home or is not in the office for any other reason and colleagues need to gain access into the office;
- 4.7 The duplicate keys of registries and other sensitive areas must be stored in a properly sealed envelope (with its details on the outside) by the Key Custodian;
- 4.8 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.

5. RESPONSIBILITIES OF THE KEY CUSTODIAN

- 5.1 Establish Key Control Register;
- 5.2 Keys to the offices must be strictly controlled;
- 5.3 The Key Custodian will be the only person authorized to do the duplication of keys;
- 5.4 No person is allowed to have the master or duplicate keys of offices except the Key Custodian;

- 5.5 The Key Custodian has to ascertain that duplicate keys are safeguarded and available for every office;
- 5.6 Duplicate keys kept for emergency purposes must be sealed and stored in the prescribed cabinet. Security Management or the higher line functional Managers are the only ones that can give permission to break a seal;
- 5.7 If a duplicate key is needed to open a particular office, a written motivation counter signed by the Supervisor shall be forwarded to the Security Services. This will apply even when an Official left his / her office keys at home;
- 5.8 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 control action by the Information Security Unit while the Office Head can implement measures to their satisfaction.
- 5.9 Information regarding all security keys shall be entered in a record book and shall be the responsibility of the Key Custodian;
- 5.10 Officials must adhere to the security measures as indicated in the Key Control Policy and procedures.

6. OFFICE SECURITY

- 6.1 Each Member is responsible to inspect their own office or area of work for signs of intrusion at the beginning of each working day. If the member notices intrusions he/ she must immediately notify the Head of the component or next senior member so that the matter can be reported to Security Services immediately;
- 6.2 Keys must never be left on the door - they must be in the possession of the person responsible for the office. This will prevent unauthorized persons from obtaining the keys;
- 6.3 The keys to filing cabinets, safes, etc. should only be handled by the user. Such keys must never be left lying around or handled by other persons;

- 6.4 Cleaning of offices should only be done during official working hours supervised by the Occupant of the office of his / her delegate;
- 6.5 The Occupants must lock their office doors when leaving the office even in short intervals or during lunchtime;
- 6.6 The office keys must never be given to cleaning personnel. The Occupant of the office is responsible for all activities taking place in their offices.

7. CAUSES OF WEAK KEY CONTROL

- 7.1 Insufficient record keeping system;
- 7.2 Bad oversight;
- 7.3 Irresponsibility by the user or person responsible for the keys;
- 7.4 Lack of knowledge regarding the dangers of weak key control;
- 7.5 An underestimation of the value of security;
- 7.6 Weak or insufficient application of personal / personnel security;
- 7.8 Laziness on the part of the user;
- 7.9 The belief by personnel that there is nothing of value in their offices, or nothing will happen;
- 7.10 Failure to adhere to security measures.

8. DANGER OF WEAK KEY CONTROL

- 8.1 Unauthorized personnel can gain access to the content of documents;
- 8.2 Theft of documents, or other items;
- 8.3 Reproduction of the content of documents;
- 8.4 Placing of explosive devices;
- 8.5 Placing of eavesdropping devices in the office, or in the telephones and intercom systems;
- 8.7 Arson;
- 8.8 Committing of acts of sabotage;
- 8.9 Tampering with content of documentation or registers, such as fraud;
- 8.10 Compromising the confidentiality of information.

9. AT THE END OF THE DAY BEFORE DEPARTURE EACH OFFICIAL SHOULD ASCERTAIN THAT:-

- 9.1 All electrical appliances are switched off;
- 9.2 Blinds, curtains are closed;
- 9.3 Doors, windows and cabinets are closed/ locked.

10. KEY CONTROL PROCEDURES

The following Key Control Procedures must be adhered to:-

11. NEWLY APPOINTED PERSONNEL

New appointees must report to Directorate Security Services (MISS) and be issued with their office keys which they must sign for in a register.

12. LOST KEYS AND CHANGING OF LOCKS

- 12.1 Report to the Directorate Security Services - they will advise on action to take;
- 12.2 Open a case or make an affidavit at the South African Police Service;
- 12.3 Written motivation has to be supplied with a case number (CR Number or Affidavit from SAPS) to the Directorate Security Services through the Supervisor. Each case will be treated on its merits;
- 12.4 Employees will be responsible for the replacement costs of their lost keys if the investigation finds that the loss is due to negligence;
- 12.5 When a key is lost, the Directorate Security Services office must investigate and record such incident in the database register and change the lock immediately;
- 12.6 No Office Occupant shall be in possession of all keys;
- 12.7 No staff member shall request a duplicate key for any Employee who is absent from duty without a written request and reasons for entering such office.

13. WHERE A PERSON LEFT THEIR KEYS AT HOME

- 13.1 Written motivation has to be supplied through his Supervisor / or Manager to Directorate Security Services;
- 13.2 The Key Custodian will open the office for them 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);
- 13.3 Employees are discouraged from leaving their keys at home.

14. WHERE A PERSON IS ON LEAVE/ SICK

- 14.1 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;
- 14.2 On arrival from sick / leave a member reports to the Key Custodian and signs for the key.

15. WHERE A PERSON RESIGNS OR IS TRANSFERRED

- 15.1 In the case where an Official resigns or is being transferred or for any reason terminating their services, the office keys must be handed / returned to the Key Custodian;
- 15.2 Where the circumstances are beyond control, for instance due to death, the Supervisor must collect the key as well as the access card from the family and submit it to the Directorate Security Services.

16. SAFE KEYS AND COMBINATIONS

- 16.1 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 are displayed on the envelope:-
 - 16.1.1 The date of sealing by affixing an official date stamp;
 - 16.1.2 Signature of member(s) sealing the envelope;
 - 16.1.3 The serial number of the relevant safe/ strong room;

- 16.1.4 The office number and location of the office in the building in which relevant safe/ strong room is situated.
- 16.2 One safe key must be handed to the Key Custodian;
- 16.3 Only a person in direct control of a safe with a combination may set the combination;
- 16.4 A previous safe combination must never be re-used;
- 16.5 The user of the safe shall ensure that the combination to a safe is changed under the following conditions:-
 - 16.5.1 Every three months;
 - 16.5.2 If someone takes over the control of the safe;
 - 16.5.3 If any indication exists that the combination has been compromised;
 - 16.5.4 If a new lock is installed.

17. LOSS OF COMBINATION / SAFE KEYS

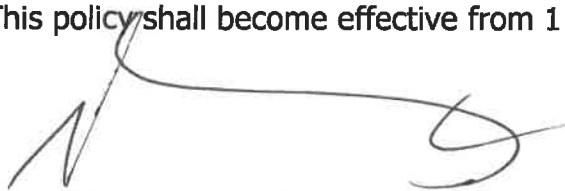
- 17.1 Where the reason for the loss of a key is not known, an investigation shall be conducted;
- 17.2 In case where the safe key combination is lost, the relevant programme shall arrange for a safe / strong room to be opened by the contractor at the programme's own cost.

18. Procedure

Refer to attached Annexure.

EFFECTIVE DATE

This policy shall become effective from 1 April 2020 and shall be reviewed annually.



MR MS THOBAKGALE
ADMINISTRATOR - DPWR

20/08/2020
DATE