



**dpwrt**

---

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

## **SECURITY MANAGEMENT POLICY**

**POLICY TITLE :       MANAGEMENT OF SECURITY POLICY**

**DEPARTMENT :       PUBLIC WORKS, ROADS AND TRANSPORT**

## **PREAMBLE**

It is the responsibility of the Department to ensure that its facilities are safe and secure for both employees and for clients.

To meet this goal, the Department needs to:

- know the security measures in place at each office and the Head Office.
- ensure that safety measures that do not meet the established standards are brought up to an acceptable level.
- conduct regular inspections to ensure that all facilities security is adequate.

## **1. DEFINITIONS AND ABBREVIATIONS**

For the purposes of this policy, the following definitions apply:

**Security authority:** a law enforcement unit - an individual or organisation to whom clients and employees should report criminal offences and whose responsibility it is to maintain the security of the facility.

**Facilities:** a complex of buildings, structures, roads and associated equipment, which represents a single management unit for financial, operational, maintenance or other purposes.

## **2. PURPOSE AND OBJECTIVES**

The purpose of this policy is to articulate the departmental guidelines regarding facilities security in order to support and enhance the delivery of services for employees and clients alike. The implementation of policy guidelines that result in safe, high-performing and secure departmental facilities shall have a direct and indirect positive impact on the working conditions of employees; on organisational performance and on service delivery.

## **3. PRINCIPLES**

### **3.1 Security**

The personal safety and security of each employee and client is both an individual and departmental concern. While the Department strives to provide an environment free of undue risks to persons and property, it is each person's responsibility to pay attention to his or her surroundings, to avoid potentially hazardous situations, and to exercise his or her own best judgment to maintain personal safety and well-being.

Each employee or client must call attention to conditions or situations which threaten the safety and security of others by contacting appropriate departmental authorities.

### **3.2 Standards of conduct and enforcement**

If any employee or visitor engages in any behaviour prohibited by this policy or by the applicable Code of Conduct, which is also a violation of local, provincial or national law or ordinance, that employee or visitor shall be subject to disciplinary procedures, where applicable, and referral to law enforcement officials for arrest and prosecution.

## **4. LEGISLATIVE FRAMEWORK**

### **4.1 Legislation**

- (a) Public Finance Management Act, Act 1 of 1999 (as amended by Act 29 of 1999)
- (b) Treasury Regulations (March 2005)
- (c) Preferential Procurement Policy Framework Act, 5 of 2000
- (d) Preferential Procurement Regulations, 2001
- (e) Broad Based Black Economic Empowerment Act, 53 of 2003
- (f) National Treasury Supply Chain Management Guidelines

### **4.2 Departmental**

- (a) Financial Management Delegations of Authority
- (b) Supply Chain Management Delegations of Authority
- (c) Departmental Policies regarding:
- (d) Occupational Health and Safety
- (e) Code of Conduct for Employees

## **5. SCOPE OF APPLICATION**

This policy applies to all departmental employees, learnership participants, interns and duly appointed cost centre managers in particular.

## **6. PROCEDURAL GUIDELINES**

### **6.1 General Security Management**

- (a) Crimes at departmental facilities shall be reported in two ways:
  - i. incident report forms submitted by members of the community with knowledge of crimes or unsafe or suspicious circumstances.
  - ii. the daily logs of facilities security officers.
- (b) Reports of security concerns should be submitted to any of the following:
  - i. a security officer
  - ii. the office manager
  - iii. the Director: Supply Chain Management
  - iv. the Chief Financial Officer.
- (c) Security officers' logs shall be reviewed by the senior SCM practitioner in the office and by the Director: Supply Chain Management. When appropriate, information describing crimes or unsafe conditions shall be posted office-wide and/or publicised through e-mail or telephone voice mail.
- (d) Although security officers have no arrest authority, they shall work very closely with the local police service.
- (e) Clients are encouraged to report crimes to the police and to utilise other services of the police services. Officers from the local police station shall be invited to train designated staff, provide statistics on local crime, and participate in forums.
- (f) Employees and visitors are subject to all local, provincial and national laws, in addition to departmental regulations. Within departmental office boundaries, the security team is responsible for enforcing those laws, although they are not sworn officers and do not have arrest powers.

## 6.2 Daily log

- (a) Departmental security shall make, keep, and update a daily log, written in a form that can be easily understood, recording all crimes reported to them. The log shall include the following information:
- i. the nature, date, time, and general location of each crime
  - ii. the disposition of the complaint, if known.
- (b) Departmental security shall record in the daily log any new information about a log entry within 24 hours after the information becomes available to it.
- (c) Generally, log entries will be open to public inspection within two business days of the initial report being made to departmental security. However, the Director: Supply Chain Management or his/her delegate, may withhold information from the log under any of the following circumstances:
- i. Where the law prohibits the Department from releasing the information
  - ii. Where releasing the information would jeopardise the confidentiality of the victim
  - iii. Where there is clear and convincing evidence that releasing the information would:
    - jeopardise an ongoing criminal investigation
    - jeopardise the safety of an individual
    - cause a suspect to flee or evade detection
    - result in the destruction of evidence.
- (d) The individual with the responsibility for determining whether information will be withheld from the log will document in writing the basis for withholding information from the log and s/he shall maintain a copy of the documentation in a secure file.

## 6.3 Gathering of crime statistics

Departmental security shall be responsible for gathering and recording the crime statistics reported to them. These statistics shall be compiled on a monthly basis and reported to the office manager for onward submission to the Director: Supply Chain Management, or his/her delegate.

## 6.4 Reporting criminal actions or other emergencies

- STEP 1** It is the policy of the Department that any criminal act; act or threat of violence; injury; destruction of departmental or personal property; traffic accident; or other situation which occurs at or in the offices of, or any other site operated by the Department, and which may constitute an emergency, a danger to the health, safety, or property of any person, or a threat to the public order be reported immediately to office security. The security officers are on duty 24 hours a day.
- STEP 2** All witnesses to any situation that fits into any of the above-described categories shall make themselves available to make written statements and otherwise assist departmental officials and police officers in the investigation of the situation. It shall be an offence subject to appropriate disciplinary action for any Department employee to file a false report or knowingly make a false statement about, or interfere with the investigation of any situation of nature described in step 1 above.
- STEP 3** It shall be the duty of the Department, upon its designated official or officials being made aware of any situation of a nature described in step 1 above, to immediately take all reasonable action to prevent or minimise any harm or threat of harm to the employees and visitors of the Department.

Furthermore it shall be the duty of said official(s) to notify the appropriate law enforcement agency in the event of an act of a criminal nature, or of any other nature (for example, a traffic accident) which would ordinarily involve law enforcement officials.

Additionally, it shall be the duty of said official(s) to contact the appropriate fire department, emergency medical agency, or other authority or agency which is due to be notified of the respective incident.

#### **6.5 Security of and access to departmental facilities**

The Department is "security conscious", and the safety of its staff and visitors is assigned a high priority. The following is a description of conditions relating to access to and security of its facilities:

- (a) All departmental facilities are open to members of the community and their invited guests. All other persons may be asked to leave or be treated as trespassers in violation of building use policies.
- (b) Employees shall be provided with access cards to facilitate smooth access to their offices and visitors shall be required to sign a register to enter the building.
- (c) Visitors arriving at and leaving the departmental offices by car shall have their boots searched to ensure that no departmental equipment leaves the premises without appropriate authority.
- (d) Outside access gates to the departmental offices shall be locked at all times and manned 24 hours a day. Buildings shall remain locked on weekends and holidays unless other events are scheduled with the approval of the Accounting Officer.
- (e) The facilities of the Department shall be lit at night.
- (f) The departmental uniformed security officers shall patrol the offices and other sites on foot.
- (g) Security officers shall submit a written report on their shift on any safety or security problems encountered.

#### **6.6 Service terminations**

It is very important to retrieve keys, access cards and other departmental equipment or resources from employees and visitors when they leave the departmental offices. Upon the termination of services of an employee, the relevant manager shall ensure that all such equipment and resources assigned to the individual are retrieved and returned to the Supply Chain Management Directorate.

This shall include, but not be limited to:

- (a) Gate access cards
- (b) Office and vehicle keys
- (c) Computer equipment (laptops)
- (d) Calculators
- (e) Electronic and hardcopy files and documents.

### **7. RESPONSIBILITIES AND OBLIGATIONS**

Overall responsibility for the implementation of this policy rests with the duly delegated Director: Supply Chain Management with implementation responsibility assigned to managers of decentralised offices.

## 8. COMMENCEMENT OF THE POLICY

This policy is effective from the signature date below.

APPROVED



---

**PJ N VAN STADEN**  
**DEPUTY DIRECTOR GENERAL**

1 September 2009

---

**Date**