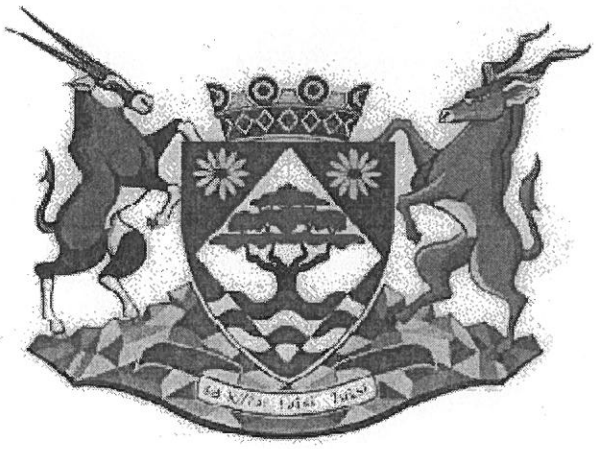
DEPARTMENT SPORTS, ARTS AND CULTURE



SECURITY POLICY

INDEX

CONFIDENTIAL

POLICY STATEMENT

The MEC, Head of Department and Management of the Department Sport, Arts and Culture believe that our employees are our greatest assets.

We are committed to creating and maintaining a relatively crime free occupational environment in which our employees have peace of mind and where service delivery is enhanced by the design, development, implementation, maintenance, evaluating and updating of a cost effective security risk management programme.

We are committed to providing reasonable resources and managerial support for a cost effective security risk management programme that is based on sound administrative and security principles, is further based on acceptable ethical standards, is within the law, is transparent, complies with the norms set out in the South African Constitution and which is compatible with values, mission strategy and corporate policy of Provincial Government/ Department of Sport, Arts and Culture of the Northern Cape

We believe that the personal involvement (Consultation with participation, co-responsibility and accountability) and the active commitment of all external and internal role players on all levels are essential if a relatively crime free working environment is to be created and maintained.

Mr. F.Aysen
HEAD OF DEPARTMENT

FRAMEWORK FOR DEPARTMENTAL SECURITY POLICY

INTRODUCTION

1. IMPLEMENTATION STEPS

- Discussion with stakeholders and affected parties within the Department
- Study of existing practices and professional standards for maintenance of security and risk prevention.

2. ADMINISTRATION

- Security Committee
- Records
- Budget

3. PHYSICAL SECURITY

- Security equipment
- Security appraisals
- Maintenance of security systems
- Other physical security needs

4. OPERATIONAL SECURITY

- Access Control
- Assets (incoming and removal)
- Departmental
- Security breaches
- Investigations
- Training
- Safes
- Private
- VIP Protection
- Firearms
- Guarding services

5. DOCUMENT SECURITY

- Registries
- Control of incoming mail
- Dispatch of mail
- Classification of documents

6. IT SECURITY

- Security System Network (Server room)
- Passwords

7. COMMUNICATION SECURITY

- Encryption

8. INFORMATION SECURITY

- Procedural document
- Security awareness programme

9. PERSONAL SECURITY

- Vetting
- Record clearance
- Oath of secrecy
- Consultants and Contractors
- Visitors to official

10. CONTINGENCY PLAN

- Disaster Management
- Fire Safety
- Contingency Plan

Areas/ Aspects/ Fields for Development

- Security division
- Physical Security
- Operational security
- Document security
- Computer security
- Information security
- Personnel security
- Communication security
- Contingency Planning

Risk preparedness and prevention

- By dismantling old policies and procedures and instituting new ones invariably alter the character of the internal working climate implementers can use the policy as a powerful changing process lever changing the corporate culture in ways that procedure fit stronger with the new strategy.

- Policies and procedures help align actions and behaviour with strategy throughout the organization, placing units on independent actions and channeling individual and group efforts along the intended path. Policies and procedures counteract tendencies for some people to resist or reject common approaches, most people refrain from violating departmental policy or ignoring established practices without first gaining clearance or having strong justification.

- Newly or freshly revised policies and procedures provide top down guidance to operating managers, supervisory personnel and employees regarding how certain things need to be done and what behaviour is expected, thus establishing some degree of regularity, stability and dependability in how management has decided to try and execute the strategy and operate the departmental business on a daily basis.

- Policies and standardized operating procedures help enforce needed consistency in how particular strategy, critical activities are performed in geographically scattered operating units (different customer service centers, regions, cultural and heritage diversity and individuals in a chain operation). Eliminating significant differences on the operating practices and procedures of organizational units performing common functions is necessary to avoid sending missed messages to internal personnel and customers who do business with the department at multiple locations.

Arts & Culture / Sport& Recreation

- Involvement with organization of large concerts and sporting events necessitates the development of strategies for crowd management and control and assessment of risks in this regard for each event organized.
- Specialist training is needed for managers and staff on the ground who are involved with such events. These two units of the Department are, more than any other involved with the movement of sports persons and artists across long distances and should be aware of the security responsibilities involved and ways to prevent risk to the State in event of claims for injuries etc. through mechanism such as the signing of indemnity forms.

Theatre /Mayibuye Centre

- Regular evacuation exercises involving users and training staff with regard to crowd control and fire safety matters are needed.

  Regular interaction with emergency services, specifically the Fire Brigade regarding safety inspections and training of staff.

Library services, Museums and Archives

- Fire and flood preparedness and training e.g. for fire ensuring that fire fighting equipment is available in critical areas and is regularly serviced and that storage containers/shelving is non-flammable etc. For flooding ensuring that basic cleanup equipment i.e. mops, squeegees, cloths and buckets are available in each storage area, ensuring that no materials are stored on the ground, etc. In these institutions there is also a need for regular meetings with emergency services agencies to ensure that they understand the specialist security and risk management needs of library, archive and museum resources and to ensure that sensitivity to these matters is built into area disaster management plans and that responsibilities under international conventions are adhered to, e.g. the Hague Convention that deals with heritage resources in times of war. (UNESCO recommends that in each community what it calls a "Blue Shield" committee be established to facilitate liaison between heritage institutions and security and risk management agencies. The International Committee of Blue Shield sets standards for risk preparedness, etc)

  Generally that inventories in the above-mentioned facilities are kept up to date in order to ensure that losses can be assessed and value apportioned.

Heritage Unit

- In terms of the National Heritage Resource Act, the Heritage Unit carries responsibility for ensuring that heritage sites and resources are properly cared for and catered for. In terms of professional standards for management of such sites, management plans must include a risk prevention and preparedness strategy. Most such sites are privately owned, but the State still has a special responsibility to ensure their safety in terms of natural and other disasters. Strategies are much the same as for libraries, archives and museums and Blue Shield standards also apply to such sites, but the State's responsibilities are shared with owners and extend principally to representing the heritage sector in disaster management formations and ensuring that disaster management agencies are familiar with the needs of heritage sites and to sensitization of owners and other parties responsible for such sites.

Need for a Security Policy

- The Arts and Culture sector is a diverse one that is made up of several different areas of practice, many of their own issues of professional practice and even legal frameworks regarding risk and security issues. Perhaps unlike many other Departments, these risk issues cannot be addressed by a general policy or ad hoc measures as the field of risk prevention and security management in the sector covered by the Department is diverse and requires its own criteria. Due to differences in practice between disciplinary areas there is a need for a policy to pull things together into a coherent whole that all stakeholders can identify with, understand and implement.

Broad Policy Outline

The policy should deal with the following:

- General considerations pertaining to security management and risk prevention in any situation, e.g. issues like identification of key personnel, establishment of a structure for management of these issues and the general safeguards and procedures applicable in all situations , e.g. access control, communications and information and records security, monitoring of systems, patrolling of areas, etc.

- Identification of specialized areas for management in the Department and details of needs, procedures and safeguards for each such situation.

- Ongoing awareness creation, training and skills development needs, including general awareness and practice as well as specialized areas.

- Establishment of liaison between professional managers in specialist areas and security and emergency/disaster management services.

- System for regular monitoring of implementation

- Schedules for servicing of equipment, evacuation and other exercises, etc.

Available resources

- Since security and risk preparedness is supposed to be an integral part of the professional practice of most of the units in the Department, unit budgets should make provision for the resources necessary to ensure implementation of a policy. If no resources necessary are included in budgets, this should be rectified in the applicable units in the future.

APPLICABLE LEGISLATION
ACTS, REGULATIONS AND DIRECTIVES APPLICABLE TO THE DEPARTMENT OF SPORT, ARTS AND CULTURE.

- Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985)
- Occupational Health and Safety Act, 1993 (Act 85 of 1993) No 181 of 1193
- Criminal Procedure Act, 1977 (Act 51 o f of 1977) *Guidelines contained in Chapter 24*
- Protection of Information Act, 1982 (Act 84 of 1982)
- Minimum Information Security Standards (MISS) policy document *(As approved in Cabinet: 4 December 1996)*
- Public Finance Management Act, 1999 (Act 1 of 1999)
- Security Officers Act, 1987 (Act 92 of 1987)
- Arms and Ammunition Act, 1969 (Act 75 of 1969) *Guidelines contained in Chapter 24*
- The trespass Act, 1959 (Act 6 of 1959)
- Labour Act: Labour relations Act of 1996 Amended 2002
- Employment Equity Act: Amended – EEA 18 of August 2006
- Access to Information Act
- Skills Development Act
- Basic Conditions of Employment
- Affirmative Action Act
- Treasury Regulations for Departments. Constitutional Institutions and Trading Entities (Government Gazette No 21249 published on 31 May 2000)
- Search Policy, Constitution of South Africa (Act 108 of 1996) Rights to privacy may be limited, Article 36
-

- Tobacco Products Control Act, 1993 (Act 83 of 1993). The Act as amended by the Tobacco Products Control Amendment Act, 1999 (Act 12 of 1999) read with Notice R975 of 2000 (Regulation Gazette 6895, Government Gazette 21610of 29 September 2000) mandated by Clause 8 of Notice R975 of 2000
- Archival Act (Act 43 of 1996)
- National Heritage Resources Act (Act 25 of 1999)
- National Sport and Recreation Act (Act 110 of 1998)
- The Cultural Affairs Act (Act 65 of 1989)
- The Museums Ordinance 8 of 1981
- National Council for library Services Act (Act 6 of 2001)
- Local Government Municipal Structures Act (Act 117 of 1998) No 44 of 2006
- White Paper on Sport and Recreation 1998
- White Paper on Arts, Culture and Heritage, 4 June 1996
- Promotion of Access to Information Act No 2 of 2000

INTRODUCTION

1. The department is continuously exposed to threats (human and natural), which can have a negative impact on the effectiveness of service delivery, should these threats not be controlled or managed properly

2. The department has to serve and protect its own interest, just like any other institution and a system of measures aimed at protecting lives, property and information is indispensable.

3. The occurrence of harmful incidents causes unnecessary losses for the Department every year. Offices increasingly fall victim to crime, which usually results in loss of or damage to property. The loss of sensitive/classified information can result in damage to and an embarrassment for the Department and/or compromise in respect of successful undisturbed operations must also be added to the list.

A. FUNDAMENTAL RESPONSIBILITIES AND ORGANISATIONAL STRUCTURE

1. At national level, the South African Police Force, the State Security Agency (SSA), the Public Service Commission and the Interdepartmental Committee entrusted with the training of Security Personnel (ICTS) are responsible for specific security functions, the last of which special mention needs to be made, because the body provides guidelines for, and is the custodian of the training of security personnel in the Public service. ICTS furthermore sets the standards of operational security services to be rendered throughout the public services and must be supported as far as possible and rendered assistance when requested to do so.

2. Within the department, the Head of Department (HOD as the Accounting Officer remains the person responsible for the orderly administration of his/her department, including security.

3. The delegated authority and responsibilities in respect of security lies with the Division: Security. Organisational structures in respect of security matter (both administrative and operational) must be put into place to perform all aspects of the specific security requirements of the department.

B. SECURITY AWARENESS

1. Developing security awareness about the protection of assets is critically important. Frequent efforts must be made to acquire conscious attention on the importance of security and the strict execution of the security programme.

2. In view of the fact that awareness for the purpose of asset protection is considered to be a single concept and that a secure environment can only be established with the full co-operation of all individuals who stake a claim to such an environment, no distinction will be made between the different levels of security awareness in the Department.

Security awareness programme's must be developed and pursued according to the guidelines provided.

C. INFORMATION SECURITY

1. Where information is exempted from disclosure, it implies that security measure will apply in full. The prescripts in this respect were compiled in accordance with the Directive: Minimum Information Security Standards (MISS) of SSA as approved by Cabinet on 4 December 1996. The need for information security measures in democratic and open society with transparency in its governmental administration according to the policy proposals regarding the intended Open Democracy Act has been taken into account.

2. The Department has valuable information that needs to be protected and the applicable security measure must be respected and meticulously adhered to

D. PHYSICAL SECURITY

1. The department values the safety of its employees as well as the property which is utilized to perform its functions, bearing in mind financial limitations for the implementation of physical security measures, more emphasis needs to be placed on staff participation to help accomplish a secure working environment. Compliance with applicable security prescripts will help to achieve the intended security objectives.

E. CONTINGENCY PLANNING

1. The purpose of contingency planning is to make provision for prevention and/or control measures aimed at saving lives, safe guarding property and information in an emergency situation, to ensure that activities can continue with as little disruption as possible.

2. A contingency plan must be drawn up and implemented according to prevailing circumstances. This plan must be practiced on a regular basis.

CONCLUSION

1. In a calculated effort to address the Department's security requirements, the above security programme aims to condition all officials to understand the relationship between security and successful operations; to know their obligation in respect of security objectives; to comply with statutory or common law requirements; to comply with regulatory requirements and to familiar with sources of help in carrying out personal and departmental responsibilities under the security programme. Compliance with the departmental security prescripts is compulsory.

2. The document serves as the departmental policy in respect of security matters and needs to be dealt with as such.

HEAD: SECURITY MANAGER