MPUMALANGA

DEPARTMENT OF CULTURE, SPORT AND

RECREATION

SECURITY POLICY

DOCUMENT INFORMATION AND LOG

File Name	Security Policy
Original Author	Department of Culture, Sport and Recreation
Review Date	2019

TABLE OF CONTENTS

1. STATEMENT OF PURPOSE

1.1. The Mpumalanga Department of Culture, Sport and Recreation depends on its personnel and assets to render effective and efficient services to the Province. It must therefore manage these resources with due diligence and take appropriate measures to protect them.

1.2 Threats that can cause harm to the department include acts of terror and sabotage, espionage, unauthorized access to the building and premise, theft, fraud and corruption, vandalism, fire, natural disaster, technical failure and accidental damage.

1.3. The security policy of Mpumalanga Department of Culture, Sport and Recreation prescribed the application security measures to reduce risk of harm that can be caused to the institution if the above can materialize. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of information and assets and ensuring the continued delivery of service to the provincial citizens.

1.4. This policy complements other Mpumalanga Department of Culture, Sport and Recreation policies (e.g. Occupational Health and Safety, Information Technology, Asset Management, Risk Management, Human and financial and resources)

2. OBJECTIVES

The core objective of this policy is to support the National interest, the Provincial interest and Mpumalanga Department of Culture, Sport and Recreation business objectives by protecting employees of the department, consultants, visitors, assets, information and ensuring the continued delivery of services to Mpumalanga citizens.

3. SCOPE OF APPLICATION

3.1. The policy is applicable to the following individuals and entities;

3.1.1 All employees of the Department and the Member of Executive Council, housed within the departmental premises and offices;

3.1.2 All contractors, and consultants delivering a service to the department, including their employees who may interact with the department;

3.1.3 temporary & contract employees, learners and interns of the department;

3.1.4 all information assets of the department;

3.1.5 all intellectual property of the department;

3.1.6 all fixed and moveable property that is owned or leased by department; and

3.1.7 all people visiting the department.

3.2 The policy further covers the following programmes of the department:

3.2.1. Security organization

3.2.2. Security Administration

3.2.3. Information security

3.2.4 Physical security

3.2.5 Personnel security

3.2.6 Information and communication technology (ICT) security.

3.2.7 Business Continuity Planning (Contingency plan)

4. PRINCIPLES

Member of Executive Council, employees, visitors, information, assets and property of the department must be protected against identified threats according to baseline (MISS) security requirements and continuous security risk management.

The Mpumalanga Department of Culture, Sport and Recreation must create a safe and secure working environment for its employees, Member of Executive Council, contractors and consultants. It must create a safe and secure environment for the public visiting the department.

Information and assets of the Mpumalanga Department of Culture, Sport and Recreation must be protected according to baseline security requirements, including business continuity planning, and continuous security risk management.

5. MANDATORY REQUIREMENTS

This policy is guided by and complies with the applicable, national legislation, national security policies (MISS DOC) and national security standards. A list of applicable regulatory documents is attached as **Annexure A.**

6. POLICY STATEMENT

6.1. General

6.1.1. Member of the Executive Council and employees of the Mpumalanga Department of Culture, Sport and Recreation must be protected against identified threats according to (MISS) baseline security requirement and continuous security risk management.

6.1.2. Information and assets of the Mpumalanga Department of Culture, Sport and Recreation must be protected according to the (MISS) baseline security requirement and continuously security risk management.

6.1.3. Continued delivery of service of the Mpumalanga Department of Culture, Sport and Recreation must be assured (through audit, assessment and TRA) and baseline security requirement, including business continuity planning and continuous security risk management.

6.2. Compliance requirements

6.2.1. All individuals mentioned in par. 3(scope of application) above must comply with the (MISS, Information Security and MPSS) baseline requirement of this policy and its associated Security Directives as contained in the Security Plan of the department. These requirements are/shall be based on integrated security Threat and Risk Assessment (TRA) to the (provincial)national interest as well as employees' information and assets of the department of Culture, Sport and Recreation. The necessity of security measures above baseline level will also be determined by continuous updating of the security TRA's at specified areas.

6.2.2. Security threat and risk assessments involve:

6.2.2.1 Establishing the scope of assessment and identifying the information, employees and assets to be protected;

6.2.2.2 Determining the threats to information, employees and assets of the Mpumalanga Department of Culture, Sport and Recreation, and assessing the probability and impact of threats occurrence by means of audit;

6.2.2.3 Assessing the risk based on the adequacy of existing security measures and vulnerabilities;

6.2.2.4 Implementing any supplementary security measures that will reduce the risk to an acceptable level

6.2.3. Staff accountability and acceptable use of assets based on assets policy.

6.2.3.1. The Security Manager and Information Security Officer shall ensure that information assets of the department are used in accordance with procedures as stipulated in the Security Policy, Assets Policy and IT Security Policy.

6.2.3.2. All employees of the Mpumalanga Department of Culture, Sport and Recreation shall be accountable for the proper utilization and protection of such information assets. Employees that misuse or abuse assets of the Department shall be held accountable therefore and disciplinary action shall be taken against such employees as per (asset management policy)

6.3. Specific baselines requirements

6.3.1. Security Organization

6.3.1.1 The Head of the Department of Culture, Sport and Recreation will appoint/ has appointed a Security Manager (SM) to establish and direct security program that ensure co-ordination of all policy functions and implementation of the policy requirements.

6.3.1.2. Given the importance of this role, Security Manager with sufficient security experience and training strategically positioned within the department shall provide a wide strategically advice and guidance to senior management and employees of an institution.

6.3.1.3. The Head of Department will ensure that the Security Manager has effective support structure (Security Component) to fulfil the functions referred in para. 6.3.2 below.

6.3.1.4. Individuals that will be appointed in the support structure of the Security Manager will all be security professionals with sufficient experience and training to effectively cope with their respective job functions.

6.3.1.5 The Security Manager will establish a Security Committee in line with the MISS document to fulfil all security requirements of the department.

6.3.1.6 The committee established shall meet on a quarterly basis to address all security operational matters of the department and compile an operational report for the Accounting Officer to be tabled during Management Meeting.

6.3.2 **Security Administration**

6.3.2.1 The function referred to in par. 6.3.1.1 above include:

6.3.2.1.1 General security administration (security policies, directives and procedures , training, workshops and awareness, security risk management (analysis and surveys), security audits and inspections, sharing information and assets)

6.3.2.1.2 Setting of access limitations

6.3.2.1.3 Administration of security screening and vetting processes

6.3.2.1.4 Implementing of physical security

6.3.2.2 Security incidents/breaches reporting process

6.3.2.2.1 Whenever an employee of the department becomes aware of an incident that might constitute a security breach or unauthorised disclosure of information (whether accidental or intentional), he/she must report that to the security manager (SM) of the department utilizing the formal procedure in the Security Breach Directives of the department. Where are those directive?

6.3.2.2.2 The Security Manager shall ensure that the Head of the Department is advised of such incidents as soon as possible.

6.3.2.2.3 The Head of Department or his/her delegate shall report to the appropriate authority all cases or suspected breaches for investigation.

6.3.2.2.4 State Security Agency (SSA) or the South African Police Services (SAPS) shall be responsible to investigate reported security breaches and provide feedback with recommendation to the department.

6.3.2.2.5 The Head of Department or his/her delegate may suspend access to classified information, assets and / or to premises until administrative, disciplinary and/or criminal process have been concluded. (Flowing from the investigations into security breaches or alleged security breaches.)

6.3.2.2.6 The Head of Department or his/her delegate may take into consideration the result of these investigations, disciplinary action or criminal action in determining to restore, revoke or limit the security access privileges of an individual or whether to revoke or alter the security clearance of an individual.

6.3.3. Information Security

6.3.3.1. Categorization of information and information classification system

6.3.3.1.1 The Security Manager must ensure that a comprehensive information classification system is developed for and implemented in the department. All sensitive information produced or processed by the department must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.

6.3.3.1.2. All sensitive information must be classified into one of the following categories:

- State Secret;
- Trade Secret; and
- Personal Information

and subsequently classified according to its level of sensitivity by using of the recognized levels of classification.

- Confidential;
- Secret; and
- Top Secret

6.3.3.1.3 Employees of the department who generate sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labelling of classified documents.

6.3.3.1.4 The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times.

6.3.3.1.5 Access to classified information will be determined by the following principles:

- Intrinsic(belonging) secrecy approach;
- Need-to-know, principle;
- Level of security clearance

6.3.3.1.6 Removal of classified information/ documents

Under no circumstances may the classified information/documents be removed from the Department without the authorisation of the Head of Department.

6.3. 4. Physical Security

6.3. 4.1. Physical security involves the proper layout and design of facilities of the department and the use of physical security measures to delay and prevent unauthorized access to assets of the department. It includes measures to detect attempted or actual unauthorized access and the activation of an appropriate response. (OHS) Physical security also includes the provision of measures to protect employees from bodily harm.

6.3. 4.2. Physical security measures must be developed, implemented and maintained in order to ensure that the entire department, its personnel, property and information are secured. These security measures shall be based on the finding of the Threat and Risk Assessment (TRA) to be conducted by the Security Manager and the Security Committee.

6.3. 4.3. The department shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities. The department shall:

- Select, design and modify facility in order to facilitate the effective control of access thereto. (have card reader machines, scanners and X-ray machine in all identified key check points in order to facilitate the effective control of access thereof;
- Demarcate restricted access areas and have the necessary entry barriers; security systems and equipment to effectively control access thereto;
- Include the necessary security specifications in planning, request for proposals and tender documentation; **(security requirement must be included in the document)**
- Incorporate related costs in funding requirements for the implementation of the above.

6.3. 4.4 The department will also ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms referred to **(IT Security policy)**

6.3. 4.5 All employees are required to comply with access control procedures of the department at all times. This includes wearing of nametags and producing of ID cards upon entering any sites of the department, the display thereof whilst on the premises and escorting of official and non-official visitors.

6.3.5. **Personnel Security**

6.3.5.1. **Security Screening**

6.3.5.1.1 Any employee, contractor and consultant who requires access to classified information and critical assets in order to perform his/her duties or functions, must be subjected to a security screening investigation conducted by the -State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

6.3.5.1.2. The level of security clearance given to a person will be determined by the content of or access to classified information entailed by the post already occupied or to be occupied in accordance with their respective responsibilities and accountability. **See Annexure C.**

6.3.5.1.3 A security clearance provides access to classified information subject to the need-to-know principles.

6.3.5.1.4 A declaration of secrecy shall be signed by every individual issued with a security clearance to complement the entire security screening process. This will remain valid even after the individual has terminated his/her services with the Department of Culture, Sport and Recreation. **(DECLARATION OF SECRECY MUST BE SIGNED EVERY YEAR)**

6.3.5.1.5 A security clearance will be valid for a period of ten years in respect of the confidential level and five years for secret and top secret. This does not preclude re-screening on a more frequent basis as determined by the Head of Department or his/her delegate, based on information, which impact negatively on an individual's security competence.

6.3.5.1.6 Security clearance in respect of all individuals who have terminated their service with the Department of Culture, Sport and Recreation shall be immediately withdrawn.

6.3.5.2. **Polygraph examination**

6.3.5.2.1 A polygraph examination shall be utilised to provide support to the security screening process. All employees subjected to a Top Secret security clearance will also be subjected to a polygraph examination. The polygraph shall only be used to determine the reliability of the information gathered during the security (vetting) investigation and does not imply any suspicious or risk on the part of the applicant.

6.3.5.2.2 In the event of any negative information being obtained with regard to the application during the security screening investigation (all levels), the applicant shall be given an opportunity to prove his/her honesty and/or innocence by making use of the polygraph examination. Refusal by the applicant to undergo the examination does not necessarily signify that a security clearance will not be granted.

6.3.5.**3. Transferability of security clearance**

6.3.5.3.1 A security clearance issued in respect of an official from other government institutions shall not be automatically transferred to the Department of Culture, Sport and Recreation. The responsibility for deciding whether the official should be re-vetted rests with the Head of the Department.

6.3.6. **Security Awareness and Training**

6.3.6.1. A security training, workshop and awareness programmes must be developed by the Security Manager and be implemented to effectively ensure that all personnel and service providers of the department remain security conscious.

6.3.6.2. All employees shall be subjected to the security awareness and training programmes and must certify that the contents of the programme(s) has been understood and will be complied with. The programme must cover training with regard to specific security responsibilities and sensitize employees and relevant contractors and consultants about the security policy and security measures of the department and the need to protect sensitive information against disclosure, loss or destruction.

6.3.6.3. Quarterly security awareness presentations, briefings, email notification and workshops will be conducted, and posters and pamphlets will be frequently distributed in order to enhance the training and awareness programme. Attendance of the above programme is compulsory for all employees identified and notified to attend the events.

6.3.6.4. Regular surveys and walkthrough inspections shall be conducted by the Security Manager and members of the security component to monitor the effectiveness of the security training and awareness programmes.

6.3.7. Information and Communication Technology (ICT) Security

6.3.7.1. ICT Security

6.3.7.1.1 A secure network shall be established for the department in order to ensure that information systems are secure against rapidly evolving threats that have the potential to impact on their confidentiality, integrity, availability, intended use and value. **See ICT security policy**

6.3.7.1.2. To prevent the compromise of ICT systems, the department shall implement baseline security controls and any additional control identified through the security Threat Risk Assessment. These controls, and the security roles and responsibilities of all personnel, shall be clearly defined, documented to all employees. See ICT security controls

6.3.7.2 Communication security

6.3.7.2.1 The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of the department in all its forms and at all times.

6.3.7.2.2 All sensitive electronic communications by employees, contractors or employees of the department must be encrypted in accordance with the South African Communication Security Agency (SACSA) standards, COMSEC standards and the Communication Security Directive of the department. Encrypted devices shall only be purchased from SACSA or COMSEC and will not be purchased from any commercial suppliers. (Applicable when installed)

6.3.7.2.3 Access to communication security equipment of the department and the handling of information transmitted and/or received by such equipment, shall be restricted to authorized personnel only (personnel with a Top Secret Clearance who successfully completed the SACSA Course). (Applicable when installed)

6.3.7.3 Technical surveillance counter measures (TSCM)

6.3.7.3.1 Identified All offices, meeting, conference and boardroom venues of the department where sensitive and classified matters are discussed on a regular basis shall be identified and shall be subjected to proper and effective physical security and access control measures. Periodic electronic Technical Surveillance Counter Measures (sweeping) will be conducted by SSA to ensure that these areas are kept sterile and secure.

6.3.7.3.2 The Security Manager of the DCSR shall ensure that areas that are used for discussions of a sensitive nature as well as offices / rooms that house electronic communications equipment are physically secured in accordance with the standards laid down by (MISS DOC) SSA. This is in order to support the sterility of the environment after TSCM examination, before any request for a TSCM examination is submitted.

6.3.8 Business Continuity Planning (BCP)

6.3.8.1 The ICT Manager or a delegated IT official and a Security Manager of the DCSR must establish a Business Continuity Plan (BCP) to provide the continued availability of critical services, information and assets if a threat materialized and to provide for appropriate steps and procedures to respond to an emergency to ensure the safety of employees, contractors, consultants and visitors. **See ICT Policy**

7. SPECIFIC RESPONSIBILITY

7.1. Head of the Institution

7.1.1 The Head of the Department of Culture, Sport and Recreation bears the overall responsibility for implementing and enforcing the security program of the department. Towards the execution of this responsibility, the Head of Department shall;

7.1.1.1 Establish the post of the Security Manager and appoint a well-trained and competent security official in the post.

7.1.1.2 Establish a security Committee for the department and ensure the participation of all senior management of the core business function of the department in the activities of the committee.

7.1.1.3 Approve and ensure compliance with this policy and its associated Security Directives by all to whom it is applicable.

7.2 Security Manager

7.2.1. The delegated security responsibility lies with the Security Manager of the Mpumalanga Department of Culture, Sport and Recreation, who will be responsible for the execution of the entire security function and program within the department (coordination, planning, implementing, controlling and etc.) towards execution of his/her responsibilities, the Security Manager shall, amongst others:

7.2.1.1 Take a role of a Chairperson in the security committee of the department.

7.2.1.2 Draft the internal Security Policy and Plan (containing the specific and detailed Security Directives) of the department in conjunction with the security committee

7.2.1.3 Review the security Policy and Security plan at regular intervals

7.2.1.4 Conduct a security TRA of department with the assistance of the security committee

7.2.1.5 Advise management on the security implication of their decisions

7.2.1.6 Implement a security awareness program

7.2.1.7 Conduct internal compliance audits and inspections in the department at intervals.

7.2.1.8 Establish a good working relationship with both State Security Agency and SAPS and liaise with these institutions on regular basis.

7.3 Security Committee

7.3.1.1 The Head of the Department shall establish a security committee for the institution and ensure the participation of all management of all the business units of the department in the activities of the committee.

7.3.1.2 The Security Committee referred to in par. 7.1.1. above shall consist of senior managers/managers of the department representing all the main business units of the department.

7.3.1.3 The responsibility of security of the department is delegated to the Security Manager, who will be responsible for the execution of the entire security function and programme within the department and therefore the Security Manager shall chair the security committee of the department.

Participation in the activities of the Security Committee by the appointed representatives of business units of the Legislature shall be compulsory.

7.3.1.4 The Security Committee shall be responsible for assisting the Security Manager in the execution of all security related responsibilities in the department, including completing tasks such as drafting/reviewing of the Security Policies and Plans, conducting of a security Threat Risk Assessment, conducting of security audits, inspections, drafting of a BCP and assisting with security awareness and training.

7.4 Line management

7.4.1 All mangers of the department shall ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of the department at all times.

7.4.2 Managers must ensure that appropriate measures are implemented and steps are taken immediately to rectify any non-compliance issues that may come to their attention. This includes the taking of disciplinary action against employees if warranted.

7.5 Employees, Consultants, Contractors and other Service Providers

7.5.1 Every employee, consultant, contractor and other service providers of the department shall know what their security responsibilities are, accept it as part of their normal job function, and not only cooperate, but contribute to improving and maintaining security in the department at all times.

8. Readership

8.1. This policy is applicable to all employees of the Department of Culture, Sport and Recreation, consultants, contactors and any other service providers of the department. It is further applicable to all visitors and members of the public visiting the premises of or may officially interact with the department.

9. Enforcement

9.1. The Head of Department, the security committee, staff in the security section and appointed Security Manager are accountable for the enforcement of this policy.

9.2. All employees of the Department of Culture, Sport and Recreation are required to comply with this policy. None-compliance with any prescripts shall be addressed in terms of the disciplinary code of the Department of Culture, Sport and Recreation.

9.3. Prescripts to ensure compliance to this policy and the security directives by all consultants, contractors or service providers of the Department shall be included in the contracts signed with such individuals/ institutions/ companies. The consequences of any transgression/deviation or none-compliance shall be clearly stipulated in the said contracts and shall be strictly enforced. Such consequences may include the payment of prescribed penalties or termination of the contract, depending on the nature of any non-compliance.

10. Exception

10.1. Deviation from this policy and its associated Security Directives will only be permitted in the following circumstances:

i. When security must be breached in order to save or protect the lives of people;

ii. During unavoidable emergency circumstances e.g. natural disasters;

iii. On written permission of the Head of Department (reasons for allowing non-compliance to one or more aspects of the policy and directives shall be clearly stated in such permission. No blanket non-compliance shall be allowed.

11. Other Consideration

11.1 The following shall be taken into consideration when implementing this policy;

11.1.1 Occupational Health and Safety issues

11.1.2 Disaster Management issues in the Department

11.1.3 Disabled person shall not be inconvenienced by physical security Measures and must be catered for in such a manner that they have access without compromising security or integrity of this policy.

11.1.4 Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on environment)

12 Communicating the policy

12. 1. The Security Manager of the department shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees. With regard consultants, contractors, service providers, clients, visitors, members of the public that may officially interact with the department the Security Manager shall conduct briefing sessions as and when they come to the department. The Security Manager will further ensure that the department complies with, as well as enforcing all security policies and directive prescriptions. The practicality in relation to service provider

12.2 The Security Manager must ensure that a comprehensive security awareness programme is developed and implemented within the Department to facilitate the above said communication. Communication of the policy by means of this programme shall be conducted as follows:

i. Awareness workshops and briefings to be attended by all employees;

ii. Distribution of memos and circulars to all employees;

iii. Access to the policy and applicable directives on the intranet of the Department.

13. Review and update process

13.1. The Security Manager, assisted by the Security Committee of the Department, must ensure that the policy and its associated security directives is reviewed and updated on an annual basis. Amendments shall be made to the policy and directives as the need arise.

14. Implementation

14.1. The Security Manager of the Department must manage the implementation process of this policy and its associated security directives (contained in the security plan) by means of an action plan (also to be included in the security plan of the Department).

14.2. Implementation of the policy and its associated security directives is the responsibility of every individual this policy is applicable to (see par. 3.1 above).

15. Monitoring of Compliance

15.1 The Security Manager, with the assistance of the security component and security committee of the Department must ensure compliance with this policy and its associated security directives by means of conducting internal security audits and inspections on a frequent basis.

15.2 The findings of the said audit inspections shall be reported to the Head of Department forthwith after completion thereof.

16. Disciplinary Action

16.1 Non-compliance with this policy and its associated security directives shall result in disciplinary action, which may include:

i. Re-training;
ii. Verbal and written warning
iii. Termination of contracts in the case of contractors or consultants delivering a service to the Department;(SECURITY REQUIREMENT ATTACHED)
iv. Dismissal;
v. Suspension;
vi. Loss of the Department information and asset resources access privileges.

16.2. Any disciplinary action taken in terms of non-compliance with this policy and its associated directives will be in accordance with the disciplinary code/directive of the Department of Culture, Sport and Recreation.

Annexure A

Applicable Legislation

1 Constitution of the Republic of South Africa, 1996 (Act 106 of 1996)
2 Protection of information Act ,1982 (Act no 84 of 1982)
3 Promotion of Access to Information Act, 2000 (Act no 2 of 2000)
4 Promotion of Administrative Justice Act, 2000 (Act no. 3 of 2000)
5 Protection of Disclosure Act, 2000 (Act 26 of 2000)
6 Copyright Act, 1978(Act no. 98 of 1978)
7 National Achieves of South Africa Act, 1996 (Act no. 43 of 1996) and regulations
8 Occupation Health and Safety Act, 1996 (Act no 85 of 1993)
9 Criminal Procedure Act, 1977, (Act 51 of 1977) as amended
10 Private Security Industry Regulatory Act, 2001 (Act 56 of 2001)
11 Control of Access to Public Premises and Vehicle Act, 1985 (Act 53 of 1985)
12 National Key Point Act, 1980 (Act 102 of 1980)
13 Trespass Act , 1959 (Act 6 of 1959)
14 Electronic Communication and Transaction Act, 2002 (Act 25 0f 2002)
15 Electronic Communication Security (Pty) Ltd Act, 2002 (Act 68 0f 2002)
16 State Information Technology Agency Act, 1998 (Act 68 of 1998)
17 Regulation of Interception of Communications Act and Provision of Communication-Related Information Act, 2002 of 2002)
18 General Intelligence Law Act,2000 (Act no. 66 of 2000)
19 National Strategic Intelligence Act 1994 (Act 39 of 1994)
20 Intelligence Service Act, 2002 (Act 65 of 2002 and regulation
21 Labour Relation Act , Act 1995 (Act 66 of 1995)
22 Employment Equity Act, 1998 (Act 55 of 1998)
23 Fire-arms Control Act, 2000 (Act 60 of 2000) and regulation
24 Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 0f 2004)
25 Public Finance Management Act,, 1999 (Act 1 of 1999) and Treasury Regulation)
26 National Building Regulation and Building Standards Act,1977 (Act 103 0f 1977)
27 Minimum Information Security Standards (MISS), second Edition March 1998
28 SACSA/090/1(4) Communication security in the RSA

Annexure B GLOSSARY AND DEFINITION

1 **"Accreditation"** means the official authorization by management for operation of the information Technology (IT) system, and acceptable by that management of the associated residual risk. Accreditation is based on the certification process as well as other management consideration;

2 **"Assets"** means material and immaterial property of an institution. Assets include but are not limited to information in all forms and stored on any media, network, or system, or material, real property, financial resources, employee trust, public confidence and international reputation;

3 **"Availability"** means the condition of being useable on demand to support operations, programs and services;

4 **"Business continuity planning"** includes the development of plan, measures, procedures and arrangement to ensure minimal or no interruption of the availability of critical service and assets;

5 **"Candidates"** means an applicant, and employee, a contract employee of a person acting on behalf of a contract appointee or independent contractor;

6 **"Certification"** means the issuing of certifying that comprehensive evaluation of the technical and non-technical security features of an Information Communication Technology system (hereinafter referred to as an "ICT" system) and its related safeguards has been undertaken and that it was established that its design and implementation meets a specific set of security requirement;

7 **"COMSEC"** means the organ of state known as Electronic Communication Security (Pty) Ltd which was established in terms of section 2 of the Electronic Communication Security Act, 2002 (Act No. 68 of 2002) and until such time as COMSEC becomes operational, the South African Communication Security Agency;

8 **"Critical service"** means a service identified by an institution as critical service through a Threat and Risk assessment and compromise of which will endanger the effective functioning of the institution;

9 **"Document"**

means:

10 any notes or writing, whether produced by hand or by printing, typewriting or any similar process, in either tangible or electronic format;
11 any copy, plan, picture, sketch or photographic or other presentation of any place or articles;
12 any disc, tape, card, perforated roll or other device in or which sound or any signal has been recorded for reproduction;

13 **"Information security"** include, but not limited to,-

- Document security;
- Physical security measure for the protection of information;
- Information and communication technology security;
- personnel security;
- business continuity planning
- security screening
- technical surveillance counter-measures;
- dealing with information security breaches; and
- administration and organization of the security function at organ of state

14 **"National Intelligent Structures"** means the National Intelligence Structures as defined in section 1 of the National Strategic Intelligent Act, Act 39 of 1994;

15 **"Reliability check"** means an investigation into criminal record, credit record and past performance of an individual or private organ of state to determine his, her or its reliability;

16 **"Risk"** means the likelihood of threat materializing by exploitation of vulnerability;

17 **"Screening investigator"** means a staff member of National Intelligence Structure designated by the head of the relevant National Intelligence Structure to conduct security clearance investigations;

18 **"Security breach"** means the negligence or intentional transgression of or failure to comply with security measures;

19 **"Security clearance"** means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subjected to the need to know;

20 **"Site access clearance"** means clearance required for access to installations critical to the national interest.

21 **"Technical Surveillance Countermeasures" (TSCM)** means the process involved in detection, localization, identification and neutralization of technical surveillance of and individual, an organ of state, facility or vehicle.

22 **"technical/ electronic surveillance"** means the interception or monitoring of sensitive or proprietary information or activities (also referred to bugging)

23 **"Threat"** means any potential event or act, deliberate or accidental, that could cause injury to a person, compromise the integrity of information or could cause a loss or damage of assets;

24 **"Threats and Risk Assessment (TRA)"** means within the context of security risk management, the process through which it is determined when to avoid, reduce and accept risk, as well as how to diminish the potential impact of threatening event;

25 "**Vulnerability**" means a deficiency related to security that could permit a threat to materialize.

ANNEXURE D
SECURITY PROCEDURES: 02 0f 2015

PHYSICAL SECURITY

1. Introduction

The provision of Control of Access to Public Premises and Vehicle Act 53 of 1985, is applicable when entering and leaving the premises of the Department. The Act gives the Head of Department for Culture, Sport and Recreation the right to give directives on how access to the Department is to be conducted. The Head of the Department delegated the function to the Security Manager. The Act also indicates that the Head of Department shall require the service of authorized officer to take over the service of access control which in this regard is the South African Police Service.

All security activity that shall be conducted by SAPS shall be based on Section 2 of the Act as well as the Criminal Procedure Act No. 51 of 1977. The Department of Culture, Sport and Recreation is one of the Mpumalanga Provincial Government Departments and therefore requires special and tactful security.

2. ACCESS CONTROL ON THE FACILITY

2.1. Issuing of access Cards

2.1.1 All persons working within the Department of Culture, Sport and Recreation, learners, interns, external auditors and contractors will be issued with access cards.

2.1.2. The Access cards serve as identification and must be complimented with the departmental nametag.

2.1.3. All the cards will be issued by SAPS at building 8. Employees must complete an access card request form obtained from a security administration officer and attach a letter of appointment and copy of ID.

2.1.4. Access card applications of newly appointed staff members must be taken to Manager: Security Management for authorization.

2.1.5 In the case of damage to an access card, the staff member must without delay submit a report explaining the circumstances under which the card was damaged to the Manager: Security Management, so that a replacement can be authorised.

2.1.6 In the case of the loss of an access card, the staff member must immediately report the loss to the member responsible for access control (Security Manager) in order to prevent another person from gaining access with that card.

2.1.7 Lost access cards that are found should be forwarded to the Manager: Security Management.

2.1.8 The staff members are responsible for the payment to be re-issued with new cards where negligence was a result of losing a card.

2.1.9 Access cards remain the property of the Department.

2.1.10 Upon notification of termination of service, transfer, or in the event of death, the relevant Manager or immediate supervisor should immediately notify the Manager: Security Management.

2.1.11 The same procedures shall apply to learners, interns, consultants or contractors employed at the Department who have been issued with access cards.

2.1.12 The supervisors under whom interns, learners, auditors, consultant or contractor render their services should ensure that the access cards and all keys are collected before the expiry dates of their contracts and be forwarded to the Manager: Security Management.

2.2. Access Control on to the facility

2.2.1. The Departmental Key Access Control Points

The Department has four key access points, which are as follows, namely:

i. The Basement personnel access control point.
ii. The Upper ground access control points.
iii. First floor access points
iv. Second floor access points

2.3. Access for employees.

2.3.1. All employees of the Department of Culture, Sport and Recreation should always use their access cards when accessing the departmental premises.

2.3.2 At each point at where access is to be controlled, access should be granted when proper identification is made available either to the mechanism (card reader system) or SAPS member and or Security Officer responsible.

2.3.3. Access cards must be carried at all times when a person is in the Departmental building.

2.3.4. If an employee has left his/her card at home he/she must register as a visitor for the day and be issued with a temporary card which must be handed back immediately when knocking off duty.

2.3.5. Management (from the level of Deputy Director upwards) will have 24 hour access to the premises.

2.3.6. All employees visiting the facility after hours must register with SAPS and Security Services at the reception and state the purpose of their visit.

2.3.7 Working over weekends and public holidays will require an official departmental letter with a Departmental Security Stamp and Recommendation. Such letters will be approved by the Head of Protection and Security Services in the Government Complex.

2.3.8 A Security Manager must be informed in writing of any extended hours to be worked during the week, weekends and public holidays.

2.3.9 All bags must be put through the X-ray Scanner Machine, and any item in bags that cannot be identified must be shown to the policy officer or security officer on duty.

2.3.10 any private property brought into the premises which could possibly be mistaken as belonging to the Department must be declared and be entered into the security registers at the main entrance. A receipt issued against the property shall be regarded as a gate release.

2.3.11 when employees leave with laptops, the security officers shall check that the person is authorized to remove the laptop, or in case of personal laptop, check the details against the release voucher to ensure that it is the same laptop that the staff member entered with.

2.4. Visitors

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

i. Contractors

ii. Consultants

iii. Service Personnel

iv. Sales Representatives

v. Job Seekers

vi. Family of staff members

2.4.2. All visitors must produce proof of identity and must be registered in the Visitors' Daily Register at the reception. The first registration shall take place at the main entrance of the Government Complex administered by the SAPS.

2.4.3. If they do not have an identity document in their possession and it is very important for them to gain access due to a sitting or any important matter they should produce any acceptable means of providing some proof of identity.

2.4.4. All visitors appointments with Senior Management must be confirmed with the relevant office first and the Security Manager must be informed of such official visits two days before the visit to make necessary security arrangements.

2.4.5. All visitors should be fetched from the security reception by the officials they are visiting and should never move within the facility without being escorted by their hosting officials and should also be escorted out of the premises.

2.4.6. An attempt should be made to assist visitors not in possession of proof of identity by calling the officials they are intending to visit or consult and to assist them at the security reception.

2.4.7. An exception to grant access to the public during sittings without proof of identity will only apply during sittings and such visitors must be directed to the boardroom and are not allowed to go into any other area except for their intended purpose.

2.4.8 The Security Officer at the reception must monitor the movement of the public during the sitting and report to the Security Manager any suspicious behaviour of the public attending the sitting.

2.5. Contractors

2.5.1. All contractors that are required to access the building on daily basis (e.g. cleaning company) must be issued with Access Card.

2.5.2. All Suppliers or contractors that do not fall in the above category should be reported to Security Manager to be cleared. The security Manager will provide a list to the Main Entrance gate and Upper ground entrances.

2.5.3. A copy of the security policy and other related or applicable policies to the contract must be given before commencing with the job.

2.5.4. All contractors should not be allowed to perform their task not being checked or left alone while in the facility.

2.5.5. Temporary cards will be issued to contractors and should be handed back after completing their task. (Applicable to contracts more than 6 months)

2.5.5. Contractors should not be allowed to work in restricted area/zones without close supervision.

2.5.6. Contractors are not allowed to carry any cameras, recording devices or any related equipment on site without the approval of the Head of the Department. Should they be found to be in possession of such articles they will be removed from the facility immediately and this must be reported to State Security Agency immediately for investigation and recommendation.

2.5.7. Fast food deliveries are not permitted to enter the facility. Prior arrangement must be made to drop and pick such at Departmental access points (upper ground, first and second floor receptions).

2.6. Access after normal business hour Hours

2.6.1. All employees returning or remaining in their offices after normal working hours must notify the Security Manager and they must be booked in and out either in the Occurrence Book or after-hour Register at the security reception.

2.6.2 Any staff member who is required to work on a week-end or public holiday, and who does not have 24 hour access, must obtain a letter to that effect from his supervisor and the letter must be authorized by the Manager: Security Services, who will forward the letter to the relevant SAPS officer. An afterhour's register need to be completed to that effect.

2.7. Vehicles.

2.7.1 All vehicles entering the Departmental premises (Government Complex) must be subject to the requirements of access control as regulated by the provisions of section 2 of the; **Control of Access to Public Premises and Vehicles Act 53 of 1985.**

2.7.2 Access control should be extended to vehicles and contents should be inspected at random on entry/exit by security personnel.

2.7.3 Only the vehicles of the MEC, the Head of Department and Chief Directors within the Department are permitted to park in building 5 Basement parking.

2.7.4 People with disability that hinders their effective movement will be granted the right to park at the basement depending on the parking availability.

2.7.5 Visitors delivering official equipment must have a delivery note or notification from the person requesting the delivery. All parcels being delivered to the premises must be delivered to the registry.

2.8. PERSONAL GOODS

2.8.1. All persons entering the Departmental premises will be required to declare at the main entrance in full any personal property which could be mistaken as the property belonging to the Department. The property must be entered in detail into the Private Property Register.

2.8.2 Such property must be accompanied by purchase invoice or a release voucher from the Security Manager to prove private ownership of the property.

2.8.3 Any property without relevant documentation will be confiscated by security officers and members of the SAPS until sufficient proof is provided.

2.9. KEY CONTROL

2.9.1 The Key Custodian **(Security Manager)** is responsible for record keeping of keys of all offices, registry and boardrooms.

2.9.2 The Key Custodian is also responsible for key control of safes and vaults as well as of combination codes of safes/vaults.

2.9.3 The Head of Department should appoint a Security Manager in writing to be a Key Custodian.

2.9.4 Any loss of keys should be reported immediately in writing to the Key Custodian after which the person responsible for access control would be informed to deal with the matter in terms of the Security Policy.

2.9.5 Duplicate keys kept for emergency use must be sealed and stored in prescribed key cabinets.

2.9.7 in case a duplicate key is needed, a written motivation counter signed by the Sectional Head or his/her delegate should be forwarded to the Security Manager. This will also be the case when a staff member left his/ her keys at home.

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

2.9.9 The Security Manager will safeguard duplicate keys and the most recent lock combinations, which must remain sealed in the envelopes in which they have been kept and stored.

2.9.10 the office keys must be returned to the Key Custodian (Security Manager) by the official who is resigning or being transferred or for any reasons terminating his/her services to the office. Where the circumstances are beyond control, for instances due to death, the supervisor must ensure the collection and return of keys.

2.9.11 Keys lost through proven negligence by the user will be the responsibility of such user to replace the entire set of keys to avoid intrusion. The duplicate keys of the new set should be handed in at the Security Manager for safekeeping. Any loss of keys should be reported in writing to the Security Manager.

3. LOSS OF EQUIPMENT

3.1 The prescribed reporting form must be completed as soon as possible and be handed in to the Security Manager of the Department.

3.2 The person reporting the asset or equipment loss must register a case with the South African Police Services within 24hrs.

3.2 The Manager: Security Management will conduct an internal investigation and/or simultaneously or at the later stage when it is necessary refer the matter to the South African Police Service or to the National Intelligence Agency for further investigation.

3.4 The security report comprising of the findings and recommendations will be submitted to the Head of Department, Sectional Head, Sectional Chief Director, Chief Operations Officer, Chief Financial Officer and Asset Manager.

4. CONTINGENCY PLANNING

4.1 All emergencies must immediately be reported to Security Manager, control room and if possible to a Departmental Emergency Management Team member.

4.2 The Security Manager, control room or a Member of Departmental emergency team must in turn report the emergency to the emergency services if necessary.

4.3 All Managers must ensure that all their subordinates are familiar with the Departmental Contingency Plan, the Business Continuity Plan and have attended the training sessions arranged by the Security Manager.

4.4 All newly appointed personnel must be familiarized with the evacuation procedures and be introduced to the relevant emergency team.

4.5 All personnel must be informed about the Emergency Coordinator, Deputy Emergency Coordinator and other functionaries on their floors.

4.6 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.

4.7 Staff members must obey instructions given by Members of the Emergency Management Team, Contingency Officers and functionaries on their floors, security personnel and emergency services on their arrival.

4.8 During an emergency all staff members must report at the assembly points indicated in an evacuation plan to enable an effective roll-call.

4.9 Lifts must not be used during emergency evacuation of the buildings.

4.10 Visitors and the people with disabilities must be assisted in case of an emergency.

5. FIREARMS

5.1 The Firearms must be declared at the main entrance and the register must be completed in full and signed by both the owner and a SAPS member.

5.2. The owner of a firearm will lock the firearm in the gun safe at the entry point before entering the premises.

5.3. As the firearm safes have two keys the owner will be requested to keep one key and a SAPS official the other. The safe cannot be opened without both keys.

5.6. This would not apply to officials of the South African Police Service and South African National Defence Force if they are on duty and visit the Department as a result of their official capacity to execute their duties.

6. OFFICE SECURITY

6.1. All staff members must be advised during induction that the Department of Culture, Sport and Recreation is not responsible for any loss or damage in respect of their own personal property.

6.2. Staff members must not leave valuable items unattended (e.g. Cellular phones, laptops, wallets, handbags). Such items should be locked away at all times when not in use. Laptops should be locked with a steel cable to the table to avoid theft.

6.3. Each member should 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 Manager immediately.

6.4 Cleaning of offices should only be done during official working hours, supervised by the occupant of the office.

6.5 Offices must be kept locked at all times when the occupant leaves the office, even for a short period of time.

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

6.7 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.

6.8 The staff member must ensure that the drafts of sensitive or classified documents are not left in the dustbins where they can be easily removed by cleaners without being shredded.

6.9 At the end of the day, before departure, each member should ascertain that:

- Electrical appliances are switched off.
- All computer systems are switched off.
- Doors, windows, safes and cabinets are locked.

7. REPORTING SECURITY INCIDENTS.

7.1 The purpose of reporting security incidents/breaches is to enable the security management to conduct internal investigation and implement effective security measures to counteract any possible threat that might hinder business operations.

7.2 Security incidents and breaches that need to be reported include:

7.2.1 Personnel trying to obtain unauthorised access into the facility or restricted areas

7.2.2 Unauthorised or improperly parked vehicles on the premises.

7.2.3 Bomb threats, hostages and any other acts threatening life or would damage property.

7.2.4 Suspicious person or activity in or in the immediate vicinity of the facility.

7.2.5 Fire, faulty electrical connections,

7.2.6 Crime that is committed by service providers, visitors and employees of the Department of Culture, Sport and Recreation e.g. theft, fraud, espionage, corruption, subversion;

7.2.7 Theft of and or loss of Departmental property whilst on the facility or in possession of employees.

7.2.8 Loss of electrical and water supply.

7.2.9 Discovery of suspicious parcels or packages;

7.2.10 Evidence of tempering with equipment, security systems, doors and locks, windows, or any access points;

7.2.11 Breach of perimeter fence.

7.2.12 Compromise of sensitive/ classified information; and

7.2.13 Compromise of IT and communication systems.

8. VISITS ABROAD BY OFFICIALS

8.1 Pre-visit planning and arrangements

8.1.1 Do not publicise your travel plans, but limit that knowledge to those who need to know.

8.1.2 Apply the following procedure regarding your documents:

- Ensure that your travel documentation (passport and visa application where necessary) are in order (at least valid for six months or above).
- Make copies of your travel documentation. It is suggested that you keep one set of copies at home and have another with you but separate from your originals.
- Memorize your passport number so you do not have to reveal your passport when filling out landing cards.
- Take extra passport photos along; this will assist in case your passport get lost or stolen.

8.2 During the visit

8.2.1 The following procedure should be applied during the visit;

- Protect your passport as theft of passports is on increase for purposes of backdoor immigration, organized crimes, terrorist actions and even espionage activities.
- Beware that government officials are especially vulnerable when travelling abroad and that officials are definite targets of the security or intelligence services of the country to be visited.
- Keep all your electronic devices safe and ensure that they are switched off after use.
- Never leave your luggage unattended as illegal substances might be placed in it or it may be stolen.
- Avoid Wi-Fi Networks as in certain Countries it is controlled or monitored by local security services.
- Avoid initiating friendship with strangers

8.3 Post visit

8.3.1 Review your system access – access that is not accounted for should be reported to the Security Manager immediately.

8.3.2 Report any unusual incidents during the visit to the Security Manager of the Department of Culture, Sport and Recreation.

8.3.3 Complete the debriefing report obtained from the Security Manager with a view to reviewing security arrangements and revising measures.

8.3.4 Complete your financial settlement as soon as possible upon return.

8.3.5 Report foreigners contacting you after returning to South Africa to the Security Manager at 013 – 7665030 and email: jjmasina@mpg.gov.za

9. DOCUMENT APPROVAL

policy was approved by the Head of Department on 30 of JANUARY 2016 at Mbombela and will bein effect upon signature

SW MNISI
HEAD;CULTURE, SPORT AND RECREATION