

DEPARTMENT OF SOCIAL DEVELOPMENT AND SPECIAL PROGRAMMES

SECURITY MANAGEMENT POLICY

POLICY REGISTRATION NO: 2013-312

TABLE OF CONTENTS

I.	PREAMBLE	1
II.	PURPOSE	2
III.	OBJECTIVES	2
IV.	SCOPE OF APPLICABILITY	2
V.	PRINCIPLES AND VALUES	3
VI.	POLICY STATEMENT	3-13
VII.	APPROVING AUTHORITY	14
VIII.	ADMINISTRATION OF THE POLICY	14
IX.	ACCOUNTABILITIES AND RESPONSIBILITIES	14-15
X.	EFFECTIVE DATE OF THE POLICY	16
XI.	PROCEDURES FOR IMPLEMENTATION	16
XII.	MONITORING OF COMPLIANCE	16
XIII.	REVIEW OF THE POLICY	17
XIV.	POLICY RECOMMENDATION AND APPROVAL	20

Oh

Definitions of Terms

I.	<p>“Accreditation” means the official authorization by management for the operation of an Information Technology (IT) system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations;</p>
II.	<p>“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, networks or systems, or materiel, real property, financial resources, employee trust, public confidence and international reputation;</p>
III.	<p>“Availability” means the condition of being usable on demand to support operations, programmes and services;</p>
IV.	<p>“Business continuity planning” includes the development of plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical services and assets;</p>
V.	<p>“Candidate” means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor;</p>
VI.	<p>“Certification” means the issuing of a certificate certifying that a comprehensive evaluation of the technical and non-technical security features of an Information and 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 requirements;</p>
VII.	<p>“Critical service” means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the institution;</p>
VIII.	<p>“Document” means -</p> <ul style="list-style-type: none"> • any note or writing, whether produced by hand or by printing, typewriting or any other similar process, in either tangible or electronic format; • any copy, plan, picture, sketch or photographic or other representation of any place or article; • any disc, tape, card, perforated roll or other device in or on which sound or any signal has • been recorded for reproduction;
IX.	<p>“Information security” includes, but is not limited to, —</p> <ul style="list-style-type: none"> • document security; • physical security measures for the protection of information; • information and communication technology security; • personnel security; • business continuity planning; • contingency planning; • security screening; • technical surveillance counter-measures; • dealing with information security breaches; • security investigations; and • administration and organization of the security function at organs of state;
X.	<p>“National Intelligence Structures” means the National Intelligence Structures as defined in section 1 of the National Strategic Intelligence Act, Act 39 of 1994;</p>
XI.	<p>“Reliability check” means an investigation into the criminal record, credit record and past performance of an individual or private organ of state to determine his, her or its</p>

" PH

	reliability;
XII.	“Risk” means the likelihood of a threat materializing by exploitation of vulnerability;
XIII.	“Screening investigator” means a staff member of a National Intelligence Structure designated by the head of the relevant National Intelligence Structure to conduct security clearance investigations;
XIV.	“Security breach” means the negligent or intentional transgression of or failure to comply with security measures;
XV.	“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 subject to the need to know;
XVI.	“Site access clearance” means clearance required for access to installations critical to the national interest;
XVII.	“Technical Surveillance Countermeasures” (TSCM) means the process involved in the detection, localization, identification and neutralization of technical surveillance of an individual, an organ of state, facility or vehicle;
XVIII.	“Technical / electronic surveillance” means the interception or monitoring of sensitive or proprietary information or activities (also referred to as “bugging”);
XIX.	“Threat” means any potential event or act, deliberate or accidental that could cause injury to persons compromise the integrity of information or could cause the loss or damage of assets;
XX.	“Threat 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 a threatening event;
XXI.	“Vulnerability” means a deficiency related to security that could permit a threat to materialize.

LEGISLATIVE FRAMEWORK	
I.	Constitution of the Republic of South Africa, 1996 (Act no 106 of 1996)
II.	Protection of Information Act, 1982 (Act no 84 of 1982)
III.	Promotion of Access to Information Act, 2000 (Act no 2 of 2000)
IV.	Promotion of Administrative Justice Act, 2000 (Act no 3 of 2000)
V.	Copyright Act, 1978 (Act no 98 of 1978)
VI.	National Archives of South Africa Act, 1996 (Act no 43 of 1996) and regulations
VII.	Public Service Act, 1994 (Act no 103 of 1994) and regulations
VIII.	Occupational Health and Safety Act, 1993 (Act no 85 of 1993)
IX.	Criminal Procedures Act, 1977, (Act no 51 of 1977), as amended.
X.	Private Security Industry Regulations Act, 2001 (Act no 56 of 2001)
XI.	Control of Access to Public Premise and Vehicles Act, 1985 (Act no 53 of 1985)
XII.	National Key Points Act, 1980 (Act no 102 of 1980)
XIII.	Trespass Act, 1959 (Act no 6 of 1959)
XIV.	Electronic Communication and Transaction Act, 2002 (Act no 25 of 2002)
XV.	Electronic Communications Security (Pty) Ltd Act, 2002 (Act no 68 of 2002)
XVI.	State Information Technology Agency Act, 1998 (Act no 88 of 1998)
XVII.	Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act no 70 of 2002)
XVIII.	General Intelligence Law Amendment Act, 2000 (Act no 66 of 2000)
XIX.	Intelligence Service Act, 2002 (Act no 65 of 2002) and regulations
XX.	National Strategic Intelligence Act, 1994 (Act no 39 of 1994)
XXI.	Intelligence Services Control Act, 1994 (Act no 40 of 1994)
XXII.	Labour Relations Act, 1995 (Act no 66 of 1995)
XXIII.	Employment Equity Act, 1998 (Act no 55 of 1998)
XXIV.	Occupational Health and Safety Act, 1993, (Act no 83 of 1993).
XXV.	Fire-arms Control Act, 2000 (Act no 60 of 2000) and regulations
XXVI.	Non-Proliferation of Weapons of Mass Destruction Act, 1993 (Act no 87 of 1993)
XXVII.	Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act no 33 of 2004)
XXVIII.	Protected Disclosures Act, 2000 (Act no 26 of 2000)
XXIX.	Intimidation Act, 1982 (Act no 72 of 1982)
XXX.	Prevention and Combating of Corrupt Activities Act, 2004 (Act no 12 of 2004)
XXXI.	Public Finance Management Act, 1999 (Act no 1 of 1999) and Treasury Regulations
	Other regulatory framework documents
1.	Minimum Information Security Standards (MISS), 1996
2.	SSA Guidance Documents: ICT Policy and Standards: Part 1 & 2
3.	International Standard of Operations 17799
4.	National Building Regulations

This policy is informed by and complies with applicable national legislation, national security policies and national security standards.

Qel

ABBREVIATIONS

BCP	Business Continuity Planning
ICT	Information and Communication Technology
IT	Information Technology
MISS	Minimum Information Security Standards
SAPS	South African Police Services
SM	Security Manager
SOCDEV	Department of Social Development and Special Programmes
SSA	State Security Agency
TRA	Threat and Risk Assessment
TSCM	Technical Surveillance Counter Measures

1. PREAMBLE

- 1.1. Departmental security is the assurance that information, assets (Human and physical) and services are protected against risks and vulnerabilities. The Department therefore depends on its personnel, information and assets to deliver services that ensure the health, safety, security and economic well- being of citizens within the Eastern Cape. 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, from within South Africa and abroad, include acts of terror and sabotage, espionage, unauthorized access to buildings and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disasters, technical failures and accidental damage. The threat of cyber-attack and malicious activity through the Internet is prevalent and can cause severe harm to electronic services and critical infrastructure. Threats to the national interest, such as transnational criminal activity, foreign intelligence activities and terrorism, continue to evolve as the result of changes in the international environment. The policy is being developed in order to increase the compliance rating to the MISS as audited by SSA and to create a secure environment for officials to operate within.
- 1.3. The world and especially South Africa has changed dramatically during the last few years, with profound implications for our society and our government. The understanding of a range of issues that impact on security is evolving. Economic and environmental issues are of increasing concern and compete with traditional political and military issues for resources and attention. The South African Government has to serve and protect its own interests just like any other sovereign state in the world. The State Security Agency (SSA) has a statutory responsibility to protect the interests of the State through counter-intelligence measures. With these imperatives in mind SSA has focused their attention on the process used to formulate and implement information security policies on a national basis. These processes used to formulate policies and deliver information security services must be sufficiently flexible to facilitate change.
 - 1.3.1. The need for secrecy and therefore information security measures in a democratic and open society with transparency in its governmental administration;
 - 1.3.2. The security standards and procedures must result in the fair and equitable treatment of those upon whom we rely to guard the security;
 - 1.3.3. Security policies must realistically match the threats against the Department and its people;
 - 1.3.4. Security policies, practices and procedures must provide the needed

information security in a cost effective way that will benefit the socio-economic development of the province.

1.4. With these aspects in mind the Minimum Information Security Standard (MISS) was compiled as an official government policy document on information security, which must be maintained by all institutions who handle sensitive/classified material of the Government. This will ensure that the Departmental information interests are protected.

1.5. The Security Policy of the Department prescribes the application of security measures through continuous assessment of risks to reduce identified harm that can be caused to the institution if these threats should materialize. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of services by implementation, monitoring and maintaining of appropriate internal management controls involving prevention (mitigation), detection, response and recovery. Since the Department relies extensively on information and communication technology (ICT) to provide its services, this policy emphasizes the need for acceptable use of ICT equipment as well as ICT protection measures to be complied with by employees.

1.6. Security Management is achieved when it is supported by top management- an integral component of strategic and operational planning and embedded into departmental frameworks, culture, day-to-day operations and employee behaviors. Security threats, risks and incidents must be proactively managed to help protect the department's critical assets, information and services.

2. PURPOSE

The purpose of this policy therefore is to support the Departments asset interests and the business objectives by protecting employees, information and assets and assuring the continued delivery of services to all citizens within the Eastern Cape.

3. OBJECTIVES

4. SCOPE OF APPLICABILITY

4.1. This policy is applicable to the following individuals and entities:

- a) Employees of the Department;
- b) Contractors and consultants delivering a service to the Department, including their employees who may interact with the Department;
- c) Temporary employees of the Department;
- d) Information assets of the Department;
- e) Intellectual property of the Department;

- f) Fixed property that is owned or leased by the Department;
- g) Moveable property that is owned or leased by the Department
- h) Visitors to any premises of the Department;
- i) Members of the public visiting premises of or may officially interact with the Department

5. PRINCIPLES AND VALUES

5.1. The following principles and values underpin this policy:

- a) **Confidentiality** (also known as secrecy), meaning that sensitive information and assets can be read only and available to authorized parties.
- b) **Integrity**, meaning that the information and assets can only be modified or deleted by authorized parties in authorized ways.
- c) **Availability**, meaning that the assets are accessible to the authorized parties in a timely manner (as determined by the systems requirements).
- d) **Accountability**, meaning that every person on whom this policy is applicable has the accountability to ensure compliance with the policy and applicable directives.
- e) **Honesty**, meaning that every person must ensure that no sensitive information or assets are being compromised in a dishonest way.
- f) **Loyalty**, means the protection of sensitive state information and assets at all times.

6. POLICY STATEMENT

6.1. General

- 6.1.1. Employees of the Department must be protected against identified threats according to baseline security requirements and continuous security risk management.
- 6.1.2. Information and assets of the Department must be protected according to baseline security requirements and continuous security risk management.
- 6.1.3. Continued delivery of services of the Department must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.
- 6.1.4. The policy further covers the following seven elements of the security program of Social Development:
 - a) Security organization
 - b) Security administration
 - c) Information security
 - d) Physical security
 - e) Personnel security

- f) Information and Communication Technology (ICT) security
- g) Business Continuity Planning (BCP).

6.2. Compliance requirements

6.2.1. All individuals mentioned in par.3.1 above must comply with the baseline requirements of this policy and its associated Security Directives as contained in the Security Plan of the Department. These requirements shall be based on integrated security Threat and Risk Assessments (TRA's) to the national interest as well as employees, information and assets of the Department. The necessity of security measures above baseline levels will also be determined by the continual updating of the security TRA's.

6.2.2. Security threat and risk assessments involve:

- a) establishing the scope of the assessment and identifying the information, employees and assets to be protected;
- b) determining the threats to information, employees and assets of the Department and assessing the probability and impact of threat occurrence;
- c) assessing the risk based on the adequacy of existing security measures and vulnerabilities;
- d) implementing any supplementary security measures that will reduce the risk to an acceptable level.

6.2.3. Staff accountability and acceptable use of assets

- a) The Head of Department of Eastern Cape Department of Social Development and Special Programmes (the Department) shall ensure that information and assets of the Department are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of the Department.
- b) All employees of the Department shall be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse assets of the Department shall be held accountable therefore and disciplinary action shall be taken against any such employee.

See Disciplinary Code

See organizational structure of security component (in security plan)

6.3. Specific baseline requirements

6.3.1. Security organization

- a) The Head of Department shall appoint a Security Manager (SM) to establish and direct a security program that ensures co-ordination of all policy functions and implementation of policy requirements.
- b) Given the importance of this role a Security Manager with sufficient security experience and training, who is strategically positioned within the Department so as to provide institution-wide strategic advice and guidance to senior management, shall be appointed.

- c) The Head of Department shall ensure that the Security Manager has an effective support structure (security component) to fulfill the functions referred to in par. 5.3.2 below.
- d) Individuals that shall be appointed in the support structure of the Security Manager shall all be security professionals with sufficient security experience and training to effectively cope with their respective job functions.

See detail functions in Security Component SOP's in Security Plan

6.3.2. Security administration

- a) The functions referred to in par. 5.3.1 above include:
 - i. general security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);
 - ii. setting of access limitations;
 - iii. administration of security screening;
 - iv. implementing physical security;
 - v. ensuring the protection of employees;
 - vi. ensuring the protection of information;
 - vii. ensuring ICT security;
 - viii. ensuring security in emergency and increased threat situations;
 - ix. facilitating business continuity planning;
 - x. ensuring security in contracting; and
 - xi. facilitating security breach reporting and investigations.

See Security Directive: Reporting of Security Breaches

b) Security incident/breaches reporting process

- i. Whenever an employee of the Department becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidentally or intentionally), he/she shall report that to the Security Manager of the Department by utilizing the formal reporting procedure prescribed in the Security Breach Directive of the Department.
- ii. The Head of Department shall report to the appropriate authority (as indicated in the Security Breach Directive of the Department) all cases or suspected cases of security breaches, for investigation.
- iii. The Security Manager of the Department shall ensure that all employees are informed about the procedure for reporting security breaches.

See Security Directive: Security Breaches Response Process

c) Security incident/breaches response process

- i. The Security Manager shall develop and implement security breach response mechanisms for the Department in order to address all security breaches/alleged breaches which are reported.
- ii. The Security Manager shall ensure that the Head of Department is

- advised of such incidents as soon as possible.
- iii. It shall be the responsibility of the National Intelligence Structures (e.g. SSA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendation to the Department.
- iv. Access privileges to classified information, assets and/or to premises may be suspended by the Head of Department until administrative, disciplinary and/or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches.
- v. The end result of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the Head of Department in determining whether to restore, or limit, the security access privileges of an individual or whether to revoke or alter the security clearance of the individual

See Security Directive:
Information Classification
Process

6.3.3. Information security

- a) **Categorization of information and information classification system**
 - i. The Security Manager shall ensure that a comprehensive information classification system is developed for and implemented in the Department. All sensitive information produced or processed by the Department shall be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.
 - ii. All sensitive Information shall be categorized into one of the following categories:
 - a) State Secret;
 - b) Trade Secret; and
 - c) Personal Information

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

- d) Confidential;
- e) Secret; and
- f) Top Secret.
- iii. Employees of the Department who generate sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This

See Security Directive:
Protection of Information:
General requirements

- responsibility includes the labeling of classified documents.
- iv. The classification assigned to documents shall be strictly adhered to and the prescribed security measures to protect such documents shall be applied at all times.
 - v. Access to classified information shall be determined by the following principles:
 - 1) intrinsic secrecy approach;
 - 2) need-to-know;
 - 3) level of security clearance.

See Security Directive:
Physical Security

6.3.4. Physical Security

- a) 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. Physical security also includes the provision of measures to protect employees from bodily harm.
- b) 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 findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Manager.
- c) 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:
 - i. select, design and modify facilities in order to facilitate the effective control of access thereto;
 - ii. demarcate restricted access areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto;
 - iii. include the necessary security specifications in planning, request for proposals and tender documentation;
 - iv. incorporate related costs in funding requirements for the implementation of the above.
- d) The Department shall also ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms.
- e) All employees are required to comply with access control procedures of the Department at all times. This includes the producing of ID Cards upon entering any sites of the Department, the display thereof whilst on the premises and the escorting of official visitors

See Security Directive:
Protection of Information:
General Requirements

See Security Directive:
Access Control

See Security Directive:
Security Screening

6.3.5. Personnel Security

a) Security Screening

- i. All employees, contractors and consultants of the Department, who requires access to classified information and critical assets in order to perform his/her duties or functions, shall be subjected to a security screening conducted by the State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.
- ii. The level of security clearance given to a person shall 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.
- iii. A security clearance provides access to classified information subject to the need-to-know principle.
- iv. 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.
- v. 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, based on information which impact negatively on an individual's security competence.
- vi. Security clearances in respect of all individuals who have terminated their services with the Department shall be immediately withdrawn.

b) Polygraph examination

- i. A polygraph examination shall be utilized to provide support to the security screening process. All employees subjected to a Top Secret security clearance shall also be subjected to a polygraph examination. The polygraph shall only be used to determine the reliability of the information gathered during the security screening investigation and does not imply any suspicion or risk on the part of the applicant
- ii. In the event of any negative information being obtained with regard to the applicant 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.

See Security Directive
Security Screening

See Security Directive:
Security Training and

c) **Transferability of security clearances**

- i. A security clearance issued in respect of an official from other government institutions shall not be automatically transferable to the Department. The responsibility for deciding whether the official should be re-screened rests with the Head of Department.

d) **Security Awareness and Training**

- i. A security training and awareness program shall be developed by the Security Manager and implemented to effectively ensure that all personnel and service providers of the Department remain security conscious.
- ii. All employees shall be subjected to the security awareness and training programs and must certify that the contents of the programs(s) has been understood and will be complied with. The program shall cover/covers 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.
- iii. Periodic security awareness presentations, briefings and workshops will be conducted as well as posters and pamphlets frequently distributed in order to enhance the training and awareness program. Attendance of the above programs is compulsory for all employees identified and notified to attend the events.
- iv. 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 program.

Awareness

See ICT Policy and Security Directive: ICT Security

6.3.6. **Information and Communication Technology (ICT) Security**

a) **IT Security**

- i. A secure network shall be established for the Department in order to ensure that information systems are secured against rapidly evolving threats that have the potential to impact on their confidentiality, integrity, availability, intended use and value.
- ii. To prevent the compromise of IT systems, the Department shall implement baseline security controls and any additional control identified through the security TRA. These controls, and the security roles and responsibilities of all personnel, shall be clearly defined, documented and communicated to all employees.
- iii. To ensure policy compliance, the IT Manager of the Department shall:
 - 1) certify that all it systems are secure after

- procurement, accredit IT systems prior to operation and comply with minimum security standards and directives;
- 2) conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis;
 - 3) periodically request assistance, review and audits from the State Security Agency (SSA) in order to get an independent assessment.
- iv. Server rooms and other related security zones where IT equipment are kept shall be secured with adequate physical security measures and strict access control shall be enforced and monitored.
 - v. Access to the resources on the network of the Department shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of the Department shall be restricted unless explicitly authorized.
 - vi. System hardware, operating and application software, the network and communication systems of the Department shall all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.
 - vii. All employees shall make use of IT systems of the Department in an acceptable manner and for business purposes only. All employees shall comply with the IT Security Directives in this regard at all times.
 - viii. The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines as reflected in the IT Security Directives. In particular, passwords shall not be shared with any other person for any reason.
 - ix. To ensure the ongoing availability of critical services, the Department shall develop IT continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.
- b) **Internet access**
- i. The IT manager of the Department, having the overall responsibility for setting up Internet access for the Department, shall ensure that the network of the Department is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Human Resources management shall ensure that all personnel with Internet access (including e- mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet.
 - ii. The IT Manager of the Department shall be responsible for controlling user access to the Internet, as well as for ensuring that

See BCP

See Security Directive:
ICT Security and ICT
Policy

See Security Directive:

- users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security breaches and incidents.
- iii. Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible computer viruses or other malicious code.
- c) **Use of laptop computers**
- i. Usage of laptop computers by employees of the Department is restricted to business purposes only and users shall be aware of, and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.
- ii. The information stored on a laptop computer of the Department shall be suitably protected at all times, in line with the protection measures prescribed in the IT Security Directive.
- iii. Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop computers at all times, in line with the protection measures prescribed in the IT Security Directive.
- d) **Communication security**
- i. 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.
- ii. All sensitive electronic communications by employees, contractors or employees of the Department must be encrypted in accordance with COMSEC standards and the Communication Security Directive of the Department. Encryption devices shall only be purchased from COMSEC and will not be purchased from commercial suppliers.
- iii. 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.
- e) **Technical surveillance counter measures (TSCM)**
- i. 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.

See Security Directive:
Secure Discussion Areas

- ii. The Security Manager of the Department shall ensure that areas that are utilized for discussions of a sensitive nature as well as offices or rooms that house electronic communications equipment, are physically secured in accordance with the standards laid down by SSA in order to support the sterility of the environment after a TSCM examination, before any request for a TSCM examination is submitted.
 - iii. No unauthorized electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of the Department is discussed. Authorization must be obtained from the Security Manager.
- f) **Business Continuity Planning (BCP)**
- i. The Security Manager of the Department must establish a Business Continuity Plan (BCP) to provide for the continued availability of critical services, information and assets if a threat materializes and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of employees, contractors, consultants and visitors.
 - ii. The BCP shall be periodically tested to ensure that the management and employees of the Department understand how it is to be executed.
 - iii. All employees of the Department shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.
 - iv. The Business Continuity Plan shall be kept up to date and re-tested periodically by the Security Manager.

See BCP

6.4. EXCEPTIONS

- 6.4.1. Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:
- a) when security must be breached in order to save or protect the lives of people;
 - b) during unavoidable emergency circumstances e.g. natural disasters;
 - c) on written permission of the Head of Department of the 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 under any circumstances).

6.5. OTHER CONSIDERATIONS

- 6.5.1. The following shall be taken into consideration when implementing this policy:
- a) Occupational Health and Safety issues in the the Department.
 - b) Disaster management at the Department.

See Security Directive:

- c) Disabled persons 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 the integrity of this policy.
- d) Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).

Security Training and Awareness

6.6. COMMUNICATING THE POLICY

- 6.6.1. The Security Manager of the Department shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees, consultants, contractors, service providers, clients, visitors, members of the public that may officially interact with the Department. The Security Manager will further ensure that all security policy and directive prescriptions are enforced and complied with.
- 6.6.2. The Security Manager shall ensure that a comprehensive security awareness program is developed and implemented within the Department to facilitate the above said communication. Communication of the policy by means of this program shall be conducted as follow
 - a) Awareness workshops and briefings to be attended by all employees;
 - b) Distribution of memos and circulars to all employees;
 - c) Access to the policy and applicable directives on the intranet of the Department

See Disciplinary Code

6.7. REVIEW AND UPDATE PROCESS

- 6.7.1. The Security Manager, assisted by the Security Committee of the Department, shall ensure that this policy and its associated Security Directives will be reviewed as the need arise. Eg. Change in Legislation or National Mandate or when the Threat and Risk status has changed. Otherwise after three years from its date of approval.

6.8. DISCIPLINARY ACTION

- 6.8.1. Non-compliance with this policy and its associated Security Directives shall result in disciplinary action which may include, but are not limited to:
 - a) re-training;
 - b) verbal and written warnings;
 - c) termination of contracts in the case of contractors or consultants delivering a service to the Department;
 - d) dismissal;
 - e) suspension;
 - f) loss of the Department information and asset resources access privileges.
- 6.8.2. 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.

7. APPROVING AUTHORITY

The Security Management Policy, on recommendation by the Head of Department, shall be approved by the Member of the Executive Council who is responsible for the Department.

8. ADMINISTRATION OF THE POLICY

- a) The Accounting Officer bears, under all circumstances, overall responsibility for the provision and maintenance of security and therefore delegate the security function to the Security Manager to ensure provision are made for the effective administration and practice of security.
- b) On advice from the Security Manager appoints Senior Managers to serve on the Security Management Committee. The Committee shall act on behalf of the Head of Department as an oversight structure in order to provide strategic guidance and advice to the Accounting Officer on Security matters.

See Security Plan for more detail.

9. ACCOUNTABILITIES AND RESPONSIBILITIES

9.1 Head of Department

The Head of Department of the Department 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:

- a) Establish the post of the Security Manager and appoint a well-trained and competent security official in the post;
- b) Establish a security committee for the institution and ensure the participation of all senior management members of all the core business functions of the Department in the activities of the committee;
- c) Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

See Security Plan for more detail

9.2 Security Manager

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

- i. Chair the security committee of the Department;
- ii. Draft the internal Security Policy and Security Plan (containing the

- specific and detailed Security Directives) of the Department in conjunction with the security committee;
- iii. Review the Security Policy and Security Plan at regular intervals;
 - iv. Conduct a security TRA of the Department with the assistance of the security committee;
 - v. Advise management on the security implications of management decisions;
 - vi. Implement a security awareness program;
 - vii. Conduct internal compliance audits and inspections at the Department at regular intervals;
 - viii. Establish a good working relationship with both SSA and SAPS and liaise with these institutions on a regular basis.

See Security Plan for more detail

9.3 Security Committee

- a) The Security Committee referred to in par. 8.1.1 above whose members shall be appointed by the Head of Department and chaired by the Security Manager shall consist of senior managers of the Department representing all the main business units of the Department.
- b) Participation in the activities of the Security Committee by the appointed representatives of business units of the Department shall be compulsory.
- c) The Security Committee of the Department shall be responsible for, amongst others:
 - i. assisting the Security Manager in the execution of all security related responsibilities at the Department, including completing tasks such as drafting/reviewing of the Security Policy and Plan, conducting of a security TRA, conducting of security audits, drafting of a BCP and assisting with security awareness and training.

See Security Plan for more detail

See Security Plan for more detail

9.4 Line Management

- a) All managers 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.
- b) Managers shall 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.

9.5 Employees, Consultants, Contractors and other Service Providers

- a) 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 at the Department at all times.

9.6 District Security Management Committee

- a) The Security Committee referred to in par. 8.1.1 above shall comprise of District Manager, Managers and Assistant Managers representing all the main business units of the Department at district level and shall act as a sub structure to the Departmental Security Committee.
- b) Represent the relevant District on the Departmental Security Management Committee;
- c) Ensure the implementation of an internal security policy as well as directives in connection therewith within the respective Districts;
- d) Ensure that Staff members and Contractors with access to sensitive information are security cleared;
- e) Implement recommendations made in terms of the risk and threat analysis in the most efficient and economical manner that will ensure that the identified security risk will be reduced to an acceptable level;
- f) Implement measures to ensure the continuous monitoring of the compliance by the District with the Minimum Information Security Standards, the internal security policy of the Department and any directives issued in connection therewith.

10 EFFECTIVE DATE OF THE POLICY

This policy shall be implemented with effect from the date of approval by the Member of the Executive Council responsible for the Department.

11 PROCEDURES FOR IMPLEMENTATION

- a) 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).
- b) All employees of the Department shall fully comply with this policy and its associated Security Directives as contained in the Security Plan. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code/Regulations of the Department
- c) 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 non-compliance shall be clearly stipulated in 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.

See Security Directive:
Security Audits and
Inspections

12 MONITORING OF COMPLIANCE

- a) 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.

- b) The findings of said audits and inspections shall be reported to the Head of Department forthwith after completion thereof.

13 REVIEW OF THE POLICY

This policy shall be reviewed every three years and whenever necessary to maintain relevance

14 POLICY RECOMMENDATION AND APPROVAL

Recommended / ~~Not recommended~~

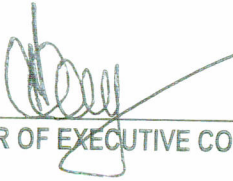


HEAD OF DEPARTMENT

2015/02/12

DATE

Approved / ~~Not approved~~



MEMBER OF EXECUTIVE COUNCIL

12/02/2015

DATE