Western Cape Government
Social Development

DEPARTMENT OF SOCIAL DEVELOPMENT (DSD) SECURITY POLICY 8/5

Approved by: Dr. Robert Macdonald

Position: Head of Department

Signature:

Date of Approval: 2016 -10- 12

Classification:

Revision date: 30 September 2017

Copy Numbers:

"Safety is everyone's responsibility"

TABLE CONTENT

GLOSSARY AND DEFINITION

- "Accreditation" means the official authorization by management for the operation of an Information Technology (IT) system, and the acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations,
- "Assets" means material and immaterial property of a department. 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,
- "availability" means the consideration of being usable on demand to support operations, programmes and services,
- "Access Control" means the process by which access to a particular area is controlled or restricted to authorized personnel only. This is synonymous with controlled access.
- "After hours" for the purpose of this policy, after hours refers to:
  (a) The time between 17:00-06:00
  (b) Saturdays and Sundays
  (c) Public Holidays
- "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,
- "candidate" means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor,
- "certification" means the issuing of a certificate 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 Its design and implementation meets a specific set of Security requirements,
- "COMSEC" means the organ of state known as Electronic Communications security (Pty) Ltd, which was established in terms of section 2 of the Electronic Communications Security Act, 2002 (Act no. 68 of 2002).
- "classification" means the grading/arrangement or re-arrangement of a document, in accordance with Its sensitivity or in compliance with security requirement,

- All official matters requiring the application of security measures (exempted from disclosure) must be classified:

  (a) Confidential relates to all information that may be used by malicious/ opposing/ hostile elements to harm the objectives and functions of individual or department.
  (b) Secret relates to all information that may be used by malicious/ opposing/ hostile elements to disrupt the objectives and functions of an individual or department
  (c) Secret relates to all information that may be used by malicious/ opposing/ hostile elements to neutralize the objectives and functions of an individual or department

- "critical services" means a service identified by an department as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the department,
- "compromise" means the unauthorized disclosure/exposure or loss of sensitive/classified information, or exposure of sensitive operations, people or place, whether by design or through negligence,
- "Computer" means that conduction created in a computer environment by the conscious provision and application of security measures. This includes information concerning the procedure for procurement and protection of equipment. Everything that could influence the confidentiality of data (an individual may have access only to that data to which he/she is suppose to), the integrity of data (data must not be tampered with and nobody may pose as another for example in the electronic mail environment, etc.) and or availability of systems is considered to be relevant to computer security.
- "Declaration of Secrecy" means an undertaking given by a person who will have, has or has had access to classified/ sensitive information, that he/she will treat such information as secret.
- "Delegation" means the transfer of authority, powers or functions from one person/department to another.
- "employees" for the purpose of this policy the term employees includes:
  Permanent staff;
  Temporary staff; and
  Contract staff.

- "premises" for the purpose of this policy, premises may refer to any building, structure, hall, room, office, land, enclosure or water surface which is the property of, or is occupied by, or is under the control of the Department of

Social Development and to which a member of the public has a right of access.

SANDF - South African National Defense Force

SAPS - South African Police Service

SASS - South African Secret Service

SSA – State security Agency

- "Visitors" mean the members of the public.
- "contractors/service providers" means any individual or company rendering a service to the NCPL, whether caterers, contractors etc.
- "Contingency planning" means the prior planning of any action that has a purpose to prevent, and to or combat, or counteract the effect and results of an emergency situation where the lives, property or information are threatened. This include compiling, approving and distributing a formal written plan and the practice thereof, in order to identify and rectify gaps in the plan and to familiarize personnel and co-ordinators with the plan.
- "document" means-
  - 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,
- "information Security" includes, but is not limited to,-
  - 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
- "National Intelligence Structures" means the National Intelligence Structures as defined in section 1 of the National Strategic Intelligence Act, Act 39 of 1994,

- "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 reliability,
- "risk means the likelihood of a threat materializing by exploitation of a vulnerability,
- "screening investigator" means a staff member of the State Security Agency designed by the head of the relevant State Security Agency to conduct Security clearance investigations,
- "Security breach" means the negligent or intentional transgression of or failure to comply with Security measures,
- "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", principle
- "site access clearance" means clearance required for access to installations critical to the national interest,
- 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,
- "technical/electronic surveillance" means the interception or monitoring of sensitive or proprietary information or activities (also referred to as "bugging"),
- "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,
- "Threat and Risk Assessment (TRA)"means, within the context of security risk management, the process through which ICT is determined when to avoid, reduce and accept risk, as well as how to diminish the potential impact of a threatening event,

  vulnerability" means a deficiency related to Security that could permit a threat to materialize,
- "WCG" means the Western Cape Government
- "SM" means Security Manager
- "SC" means Security Committee
- "DOSD" means Department of Social Development
- "SG" means Superintendent General
- "WCTSSMF" means
- "MOU" means
- "TOR" means

POLICY

1. STATEMENT OF PURPOSE

1.1 The Department of Social Development depends on its personnel, information and assets to deliver services that ensure the safety and security of all its employees. It must therefore manage these resources with due diligence and take appropriate security measures to protect them. The Public Finance Management Act (PFMA), 1999, prescribes that the Accounting Officer for a department must ensure that the department has and maintains an effective, efficient and transparent system of risk management.

1.2 Threats (man made and natural) that can cause harm to Department of Social Development include acts of sabotage, 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 have a negative impact on the workforce's effectiveness to deliver, should these threats not be controlled or managed properly.

1.3 The Security Policy of the Department of Social Development prescribes the application of security measures to reduce the risk of harm that can be caused to the department if the above 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. Since the Department of Social Development 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.

1.4 The main objective of this policy therefore is to support the interest of the Department of Social Development business objectives by protecting employees, information and assets and assuring the continued delivery of services.

1.5 This policy compliments other Department of Social Development's policies (e.g. occupational health and safety, official languages, information management, asset control, real property and financial resources).

2. SCOPE

2.1 This policy applies to the following individuals and entities:

All employees and visitors, contractors and consultants rendering a service including their employees who may interact, temporary employees, all information assets, all intellectual property, all fixed property that is owned or leased, and all moveable property that is owned or leased by the Department of Social Development.

2.2 The policy further covers the following seven elements of the Security program of Department of Social Development:

- Security Organization
- Security Administration
- Information Security
- Physical Security
- Personnel Security
- Information and Communication Technology (ICT) Security
- Business Continuity Planning (BCP)

3. LEGISLATIVE AND STATUTORY REQUIREMENTS

This policy is informed by and complies with applicable national legislation and national Security Standards. A list of applicable regulatory documents in this regard has been attached as Appendix A.

4. POLICY STATEMENT

4.1 General

4.1.1 Department of Social Development is responsible to manage public assets, personnel and information in an accountable, responsible and transparent manner, which includes identifying, addressing and appropriately managing any threats that is exposed to.

4.1.2 Employees of the Department of Social Development must be protected against identified threats according to baseline Security requirements and continuous Security Risk Management.

4.1.3 Information and assets of baseline Security requirements and continuous Security Risk Management.

4.1.4 Continued delivery of services of the Department of Social Development must be assured through baseline Security requirements, including business continuity planning, and continuous Security Risk Management.

4.2 Compliance requirements

4.2.1 All individuals and entities mentioned in Para 4.1 must comply with the base line requirements of this policy and ICT's associated Security Directives as contained in the Security plan of the Department of Social Development. These requirement are/may be based on integrated Security Threat and Risk Assessment (TRA's) to the national interest as well as employees, information and assets of the Department of Social Development. The necessity of Security measures above baseline levels will also be determined by continued updating of Security TRA's.

4.2.2 Security Threats and Risk Assessment involve:

- Establishing the scope of the assessment and identifying the information, employees and assets to be protected,
- Determining the threats to information, employees and assets of the Department of Social Development and assessing the probability and impact of threat occurrence,
- Assessing the risk based on adequacy of existing security measures an vulnerabilities
- Implementation any supplementary security measures that will reduce the risk to an acceptable level.

4.2.3 Staff accountability and acceptable use of assets

4.2.3.1 The Head of Department of Social Development as the Accounting officer will delegate to the Chief Director: Service Delivery and Co-ordination to 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.

4.2.3.2 All employees of Department of Social Development may be accountable for utilization and protection of such information and assets. Employees that misuse or abuse assets of the Department of Social Development as well as leakages of

information through negligence or malice may be held accountable therefore and disciplinary actions may be taken against any such employee.

4.3. Specific baseline requirements

4.3.1 Security Organization

4.3.1.1 The Head of Department's Designated Official, Chief Director: Service Delivery and Co-ordination of the Department of Social Development will deploy a Security Facilitator to assist with the establishment, implementation and direct a Security program that ensures co-ordination of all policy functions and implementation of policy requirements.

4.3.1.2 Given the importance of this role, a Security Facilitator (SF) with sufficient Security experience and training will be deployed in the Department of Social Development so as to provide strategic advice and guidance to senior management. In other words, the Security Facilitator may have direct access to his or her manager in matters related to the management of Security at the department concerned.

4.3.2 Security Administration

4.3.2.1 The functions referred to in Para 4.3.1 above includes:

General Security administration (departmental directives and procedures, training and awareness, Security risk management, Security audits, sharing information and assets)

- Setting access limitations
- Implementing physical Security
- Administration of Security screening
- Ensuring the protection of employees
- Ensuring the protection of information
- Ensuring ICT Security
- Ensuring Security emergency and increased threat situations
- Facilitating business continuity planning
- Ensuring Security in contracting and
- Facilitating reporting of Security breaches and investigations.

4.3.2.2 **Security incident/breaches reporting process**

4.3.2.2.1 Whenever an employee of the Department of Social Development becomes aware of an incident that might constitute a security breach or an unauthorized disclosure of information (whether accidental or intentional) the official may report that to the Security Facilitator by utilizing the formal reporting procedure prescribed in the Security Breach Directive.

4.3.2.2.2 The Head of Department's Designated Official: Chief Director: Social Welfare may report to the HOD of Social Development, State Security and SAPS all cases or suspected cases of Security breaches for investigations.

4.3.2.2.3 The Security Facilitator of the Department of Social Development may ensure that all employees are informed about the procedure for reporting security breaches.

4.3.2.3 **Security incident/breaches response process**

4.3.2.3.1 The Security Committee may develop and implement Security breach response mechanisms for the Department of Social Development in order to address all Security breaches/alleged breaches which are reported and detected.

4.3.2.3.2 The Security Facilitator may ensure that the HOD of Social Development is advised of such incidents as soon as possible.

4.3.2.3.3 IT may be the responsibility of the State Security Structures (e.g. State Security or SAPS) to conduct an investigation on reported and detected security breaches and provide feedback and in case of State Security make recommendations to the Department of Social Development.

4.3.2.3.4 Access privileges to classified documentation, assets and/or premises may be suspended by the HOD of Social Development until administrative, disciplinary and/or criminal processes have been concluded, flowing from investigations into Security breaches or alleged Security breaches.

4.3.2.3.5 The end result of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the HOD of Social Development in determining whether to restore, or limit, the security access privilege of an individual or whether to revoke or alter the Security clearance of the individual.

4.3.3 **Information Security**

The Department of Social Development has valuable information that needs to be protected; therefore applicable Security measures must be respected and meticulously adhered to. ICT is the responsibility of the Line Facilitators and staff members to ensure that where information is exempted from disclosure, Security measures are applied. The provisions of the Minimum Information Security Standard (MISS) approved by Cabinet on the 4 December 1996 may apply. All members of the department are subjected by law on disclosure of official information (Law No 84 of 1982).

4.3.3.1 Categorization of information and information classification system

4.3.3.2 The Security Facilitator in conjunction with State Security must ensure that a comprehensive information classification system is developed for and implemented in the Department of Social Development. All sensitive information produced or processed by the Department of Social Development must be identified, categorized and classified according to the origin of Its source, contents and to Its sensitivity to loss or disclosure.

4.3.3.3 All sensitive information must be categorized into one of the following categories:

- State Secret,
- Trade Secret and
- Personal Information

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

- Confidential,
- Secret
- Top Secret

4.3.3.4 Employees of the Department of Social Development who generate sensitive information are responsible to determine information classification levels and the classification thereof, subject to management review. This responsibility includes the labeling of classified documents.

4.3.3.5 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.

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

- Intrinsic secrecy approach,
- Need-to-know,
- Level of Security clearance

4.3.4. **Physical Security**

4.3.4.1 Physical Security involves the proper layout and design of offices/facilities of the Department of Social Development and the use of the 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.

4.3.4.2 Physical Security measures must be developed, implemented and maintained in order to ensure that the entire Department of Social Development, it's personnel, property and information are secured. These security measures may be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Facilitator.

4.3.4.3 The Department of Social Development may ensure that the physical Security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities as well as :

- Select, design and modify offices/facilities in order to facilitate the effective control of access thereto.
- Demarcate restricted access (zoning) areas and have the necessary entry barriers (turnstiles, paraplegic gate) , Security systems (electronic card reader) and equipment (hand metal detectors, x-ray machine) to effectively control access thereto,
- Include the necessary Security specifications in planning, request for proposals and bid documentation,
- Incorporate related costs in funding requirements for the implementation of the above.

4.3.4.4 The Department of Social Development 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.

4.3.4.5 All employees are required to comply with access control procedures of the Department of Social Development at all times. This includes the producing of ID cards upon entering any sites of the Department of Social Development, the display thereof whilst on the premises and the escorting of official visitors.

4.3.5 **Personnel Security**

4.3.5.1 **Personnel Screening**

4.3.5.1 The aim of personnel Security is to protect members of the Department against undermining influences. Members must understand why it is necessary for personnel Security to be applied. This aspect is indicated by the term personal Security, which goes hand in hand with personnel security

4.3.5.1.1 All employees, contractors and consultants of the Department of Social Development need to be screened through an evaluation process that involves the comparison and analysis of information obtained from a variety of database with the purpose of reaching a conclusion that would determine the risk value of a person or a company. A Security screening does not constitute a Security clearance and is valid for not more than 12 months, furthermore Security screening clearance does not entitle access to classified material or classified installations, however, information will be provided on a need – to - know principle.

4.3.5.1.2 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 in accordance with their respective responsibility and accountability.

4.3.5.1.3 Security vetting is a systematic investigation process undertaken to establish a person's Security competence from counterintelligence, espionage, sabotage, subversion, acts endangering Security and terrorism point of view.

4.3.5.1.4 A Declaration of secrecy may be signed by all employees, contractors and Service providers to complement the entire Security screening process. This will remain valid even after termination of services with the Department of Social Development.

4.3.5.1.5 A Security clearance will be valid for a period of ten years in respect of the Confidential level and five years respectively for Secret and Top Secret. This does not preclude re-screening on a more frequent basis as determined by the Head of Department: Social Development, based on the information which impact negatively on an individual's Security competence.

4.3.5.1.6 Security clearances in respect of all individuals who have terminated their services with the Department of Social Development may be immediately withdrawn.

4.3.5.1.7 All short listed candidates for possible appointment in the Department of Social Development may be subjected to pre - employment screening. Pre - employment screening may be conducted before interviews. In collaboration with the DOTP.

4.3.5.2 **Polygraph examination**

4.3.5.2.1 A polygraph examination may be utilized to provide support to the Security vetting process. All employees subjected to a Top Secret Security clearance will be subjected to a polygraph examination. Polygraph examination can still be used in secret Security clearance if it is deemed necessary by the State Security Officials to be used as a tool.

4.3.5.2.2 In the event of any negative information being obtained with regard to the applicant during the security vetting investigation (all levels), the applicant may be given an opportunity to prove his/her honesty and/or innocence by making use of the polygraph examination.

4.3.5.3 **Transferability of Security clearances**

4.3.5.3.1 A security clearance issued in respect of an official from other government departments may not be transferable to the Department of Social Development.

4.3.5.4 **Security Awareness and Training**

4.3.5.4.1 A Security awareness and training program must be developed by the Security Facilitator and implemented to effectively ensure that all personnel and service providers of the Department of Social Development remain security conscious.

4.3.5.4.2 All employees may be subjected to the security awareness and training programs and must certify that the contents of the program(s) has been understood and will be complied with. The program 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 of Social Development and the need to protect sensitive information against disclosure, loss or destruction.

4.3.5.4.3 Periodic Security awareness presentations, briefings and workshops will be conducted as well as posters and pamphlets frequently distributed in order to enhance the training awareness program. Attendance of the above programs is compulsory for all employees identified and notified to attend the events.

4.3.5.4.4 Regular surveys and walkthrough inspections will be conducted by the Security Facilitator to monitor the effectiveness of the security awareness and training program.

4.3.6 Information and Communication Technology (ICT) Security

4.3.6.1 IT Security

4.3.6.1.1 A security network may be established for the Department of Social Development in order to ensure that information systems are secured against rapidly evolving threats that have the potential to impact on the confidentiality, integrity availability, intended use and value. The formulation of policies with regard to Information Technology System Security rests with E. Innovation (PGWC)

4.3.6.1.2 To prevent the compromise of IT systems, the Department of Social Development may implement baseline security controls and any additional controls identified through the security TRA. These controls, and the security roles and responsibilities of all personnel, may be clearly defined, documented and communicated to all employees.

4.3.6.1.3 To ensure policy compliance, the ICT Facilitator of the Department of Social Development may :

- Certify that all IT systems are secure after procurement, accredit IT systems prior to operation and comply with minimum security standards and directives.
- Conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis.
- Periodically request assistance, review and audits from the State Security (NIA) in order to get an independent assessment.

4.3.6.1.4 Server rooms and other related security zones where IT equipment are kept may be secured with adequate security measures and strict access control may be enforced and monitored.

4.3.6.1.5 Access to the resources on the network of the Department of Social Development may be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of the departments may be restricted unless explicitly authorized.

4.3.6.1.6 System hardware, operating and application software, the network and communication systems of the Department of Social Development may all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

4.3.6.1.7 All employees may make use of IT systems of the department in an acceptable manner and for business purposes only. All employees must comply with the IT Security Directives in this regard at all times

4.3.6.1.8 The selection of passwords, their use and management as a primary means of access to systems is to strictly adhere to best practice guidelines as reflected in the IT Security Directives; in particular, passwords may not be shared with any other person for any reason.

4.3.6.1.9 To ensure the ongoing availability of critical services, the department may develop IT continuity plans as part of the overall Business Continuity Planning (BCP) and recovery activities.

4.3.6.1.10 Chief Director Security Risk Management, State Security (NIA) and Electronic Communications Security (Pty) Ltd(Comsec) may be approached for further advice and guidance in respect of Communication and computer Security needs. All Security breaches in the computer environment may be reported immediately to State Security through the correct channels.

4.3.6.2 **Internet Access**

4.3.6.2.1 The ICT Facilitator of e-Innovation (PGWC), is having the overall responsibility for setting up Internet access for the Provincial Government Western Cape (PGWC), may ensure that the network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Knowledge management may

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.

4.3.6.2.2 The IT Facilitator of the department may be responsible for controlling user access to the Internet, as well as ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information security Breaches and incidents.

4.3.6.2.3 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.

4.3.6.3 **Use of Laptop Computers**

4.3.6.3.1 Usage of laptop and computers by employees of the Department of Social Development is restricted to business purposes only, and users may be aware of and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.

4.3.6.3.2 The information stored on a laptop and computer of the Department of Social Development may be suitably protected at all times, in line with the protection measures prescribed in the IT Security Directive.

4.3.6.3.3 Employees may also be responsible for implementing the appropriate security measures for the physical protection of laptop and computers at all times, inline with the protection measures prescribed in the ICT Security Directives.

4.3.6.4 **Communication Security**

4.3.6.4.1 The application of appropriate security measures may be instituted in order to protect all sensitive and confidential communication of the Department of Social Development in all Its forms and at all times.

4.3.6.4.2 All sensitive electronic communication equipments by employees, contractors or employees of the Department of Social Development must be encrypted in accordance with the COMSEC standards and the Communication Security Directive of the Department of Social Development. Encryption devices may only be purchased from COMSEC and will not be purchased from commercial suppliers.

4.3.6.4.3 Access to communication security equipment of the Department of Social Development and the handling of information transmitted and/or received by such equipment, may be restricted to authorized personnel only.

4.3.6.5 Technical Surveillance Counter Measures (TSCM)

4.3.6.5.1 All offices, meeting, conference and boardroom venues of the Department of Social Development where sensitive and classified matters are discussed on a regular basis may be identified and may be subjected to proper and effective physical security and access control measures. Key and access control to these areas must be applied. No unauthorized electronic devices (Cell phones) may be allowed in any Boardrooms and conference facilities where sensitive information is discussed. The need for TSCM services may be directed to Chief Director Security Risk Management. Periodic electronic Technical Surveillance Counter Measures (sweeping) will be conducted by the State Security (NIA) to ensure that theses areas are kept sterile and secure.

4.3.6.5.2. The Security Facilitator of the Department of Social Development may ensure that areas that are utilized for discussion 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 the State Security (NIA) in order to support the sterility of the environment after a TSCM examination, before any request for a TSCM is submitted.

4.3.6.5.3 No unauthorized electronic devices may be allowed in any boardrooms and conference facilities where sensitive information of the Department of Social Development is discussed. Authorization must be obtained from the Security Facilitator.

4.3.7 Business Continuity Planning (BCP)

4.3.7.1 The Security Facilitator in conjunction with the Security Committee (SC) of the Department of Social Development 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 the employees, contractors, consultants and visitors.

4.3.7.2 The BCP may be periodically tested to ensure that the management and employees of the Department of Social Development understand how IT is to be executed.

4.3.7.3 All employees of the Department of Social Development may be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.

4.3.7.4 The Business continuity Plan may be kept up to date and re-tested periodically by the Security Facilitator.

5. SPECIFIC RESPONSIBILITIES

5.1 Head of Department

- The Head Of Department: Social Development bears the overall responsibility for implementing and enforcing the security program of the Department, towards the execution of this responsibility, the HOD may appoint a SMS member responsibility to the Chief Director: Service Delivery and Co-ordination who will :

- Ensure establishment of a Security Committee for the Department of Social Development and the participation of all senior management, members of all the core business functions of the Department in the activities of the Committee. The Security manage Chief Director: Service Delivery and Co-ordination chair the Security Committee meetings of the Department of Social Development
- Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.

5.2 Security Facilitator

5.2.1 The delegated security responsibilities lie with the Security Facilitator of the Department of Social Development who will be responsible for the execution of the entire security function and program of the Department of Social Development (coordination, planning, implementation, controlling, etc). Towards execution of his/her responsibilities, the Security Facilitator may , amongst other:

DD- SRM will co-ordinate matter on behalf of the DOCS-SRM

- Be a member of the security committee of the Department of Social Development,

- Draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives) of the Department of Social Development in conjunction with the Security Committee.
- Review the Security Policy and Security Plan at regular intervals,
- Conduct a Security TRA of the Department of Social Development with the assistance of the Security Committee,
- Advise management on the Security implication of management decisions and assist with physical security assistance during events arranged by the department,
- Implement a security awareness program,
- Conduct internal compliance audits and inspection at department on regular intervals, and
- Establish a good working relationship with both the SAPS and the State Security (NIA) and liaise with these Departments on a regular basis.

5.3 Security Committee

5.3.1 The Security Committee referred to in paragraph 5.1.1 above may consist of senior Facilitators or a delegated official of the Department of Social Development representing all the main business units of the department.

5.3.2 Participation in the activities of the Security Committee by the appointed representatives of business units in the Department of Social Development may be compulsory.

5.3.3 The Security Committee of the Department of Social Development may be responsible for, amongst others:

5.3.4. Assisting the Security Facilitator in the execution of all security related responsibilities of the Department of Social Development, 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.

5.4. Line Management

5.4.1 All line Managers of the Department of Social Development may ensure that their subordinates comply with this policy and the Security Directives as contained in the Security Plan of the Department of Social Development.

5.4.2 Facilitators 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.

5.5. Employees, Contractors, Consultants and other Service Providers

Every employee, Contractor, Consultant and other Service Providers of the Department of Social Development may 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 of Social.

6. STAKEHOLDERS/AUDIENCE

6.1 This policy is applicable to all members of the management, employees, consultants, contractors and any other service provider of the Department of Social Development. It is further applicable to all visitors and members of the public visiting premises of or may officially interact with the Department of Social Development.

7. ENFORCEMENT

7.1 The HOD of the Department of Social Development and the deployed Security Facilitator are accountable for the enforcement of this policy.

7.2 All employees of the Department of Social Development are required to fully comply with this policy and it's associated Security Directives as contained in the Security Plan. Non-compliance with any prescript may be addressed in terms of the Disciplinary Code/Regulations of the Department of Social Development.

7.3 Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of the Department of Social Development may be included in the contracts with such individual/department/companies. The consequences of any transgression/deviation or non-compliance may be clearly stipulated in the said contract and may 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.

8. EXCEPTIONS

8.1 Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:

- When Security must be breached in order to save or protect the lives of people,
- During unavoidable emergency circumstances e.g. natural disasters,
- On written permission of the Head of Department: Social Development (reasons for allowing non-compliance to one or more of the policy and directives may be clearly stated in such permission, no blanket non-compliance may be allowed under any circumstances.

9. OTHER CONSIDERATIONS

9.1 The following may be taken into consideration when implementing this policy:

9.1.1 Occupational Health and Safety issues in the Department of Social Development

9.1.2 Disaster Management at the Department of Social Development

9.1.3 Disabled persons may 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.

9.1.4 Environmental issues as prescribed and regulated in relevant legislation (e.g. w.. n implementing physical security measures that may impact on the environment)

9.1.5 Members of South African Police Services (SAPS), South African National Defense Force (SANDF) as well as other Security Agencies may not be subjected to searching, when they are entering on official purpose, however, they should identify themselves positively.

10. DUTIES AND FUNCTIONS OF THE OFFICE/FACILITY FACILITATOR/ DELEGATED OFFICIAL

10.1 **Periodic checks**: The Department and/or its appointed Project Facilitator may carry out periodic checks (the intervals to be determined by Regional , Local Office/facility) the purpose of which may be to determine whether service provider is providing the services in accordance with the terms and conditions of the contract if accepted by Regional, Local Office/Facility.

10.2 **Service complaints**: All service complaints, deviations, non-conforming services and suggestions that are reported to service provider by Department, its appointed facilities Facilitator, or any other party may be given proper and speedy consideration by the service provider. The service provider may investigate complaints, deviations and non-conforming services in accordance with procedures approved by the Department / Regional/ Local Office/Facility.

10.3 **User satisfaction survey:** A user satisfaction survey may be conducted by Department/ Regional/ Local Office/Facility at such intervals as Department/ Regional/ Local Office/Facility may determine to assess service user satisfaction. The user satisfaction survey may be conducted in such form and in accordance with such procedures as the parties may agree to in writing from time to time.

10.4 **Results of checks, audits and surveys:** Department/ Regional/ Local Office/Facility may be entitled to utilize the findings of the surveys, checks, audits and reports contemplated above to determine compliance by service provider with the service standards and responsibilities stipulated in the contract. It is recorded that the results of the above checks may , save to the extent that service provider can prove otherwise be binding on contractor and Department / Regional/ Local Office/Facility may be entitled to exercise its remedies stipulated in the contract based on such findings.

10.5 **Penalties:** Penalties that are stipulated in the contract agreement must be strictly applied should the service provider not adhere to these agreement.

The regional manager/local manager/ facility manager must appoint a security administrator in writing to oversee the security function at the office/facility. Contract administration must be applied at all offices and facilities.

11. COMMUNICATING THE POLICY

11.1 Security Facilitator and Security Committee may ensure that the content of the policy is communicated to all employees, consultants, visitors, service providers and members of public that interact with Department of Social Development.

11.2 The Security Facilitator must ensure comprehensive Security awareness program is developed and implemented within the Department of Social Development to facilitate communication. Communication of this policy by means of this program may be conducted as follows:

- Awareness workshop and briefings to be attended by all employees,
- Distribution of memorandums and circulars to all employees,
- Access to the policy and applicable directives on intranet of Department of Social Development

12. REVIEW AND UPDATE PROCESS

12.1 The Security Facilitator , assisted by the Security Committee of the Department of Social Development, must ensure that this policy and its associated Security Directives is reviewed and updated on an annual basis. Amendments may be made to the policy and directives as the need arise.

13. IMPLEMENTATION

13.1 The Security Facilitator of the Department of Social Development 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).

13.2 Implementation of the policy and its associated Security Directives is the responsibility of each and every individual this policy is applicable to (See par.2.1)

14. MONITORING OF COMPLIANCE

14.1 The Security Facilitator and Security Committee of the Department of Social Development must ensure compliance with this policy and it's associated Security

Directives by means of conducting internal security audits and inspections on a frequent basis.

14.2 The findings of the audits and inspections may be reported to the Head of Department of Social Development forthwith after completion thereof, which findings will determine the way forward for State Security (NIA).

15. DISCIPLINARY ACTION

15.1 Non-compliance with this policy and Its associated Security Directives may result in disciplinary action which include, but are not limited to:

- Re-training,
- Verbal and written warning,
- Termination of contracts in the case of contracts or consultants delivering a service to the Department of Social Development,
- Dismissal,
- Suspension, and
- Loss of the Department of Social Development's information and asset resources access privileges.

15.2 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 Social Development.

	ANNEXURE A: APPLICABLE LEGISLATION AND OTHER REGULATORY FRAMEWORK DOCUMENTS

1.	Constitution of the Republic of South Africa, (Act no. 108 of 1996)
2.	Public Service Act of 1994 (Act no. 103 of 1994) and regulations
3.	Copyright Act, 1978 (Act no 98 of 1978)
4.	National Archives of South Africa Act, 1996 (Act no. 43 of 1996) and regulations
5.	Promotion of Administrative Justice Act, 2000(Act 3 of 2000)
6.	Control of Access to Public Premises and Vehicle, 1985 (Act No. 53 of 1985)
7.	Protection of Information Act No. (84 of 1982)
8.	Trespass Act, 1959 (Act no. 6of 1959)
9.	Criminal Procedure Act, 1977(Act no. 51 of 1977), as amended
10.	Intelligence Service Act No. 38 of 1994
11.	Promotion of Access to Information Act No. 2 of 2000
12.	Private Security Industry Regulations Act, 2001 (Act 56 of 2001)
13.	Civil Protection Act No. 67 of 1977
14.	Electronic Communications and Transaction Act, 2002 (Act 25 of 2002)
15.	Arms and Ammunition Act No. 75 of 1969
16.	Occupational Health and Safety Act, 1993 (Act no. 83 of 1993)
17.	Public Finance Management Act No. 1 of 1999
18.	State Information Technology Agency Act, 1998 (Act 88 of 1998)
19.	Regulation of Interception of Communications and Provision of Communication – Related Information Act, 2002 (Act 70 of 2002)
20.	Fire Brigade Act No. 99 of 1987
21.	Basic Conditions of Employment Act No. 75 of 1997
22.	Compensation for Occupational Injuries and Diseases Act No. 61 of 1997
23.	Labour Relations Act, 1995 (Act no. 66 of 1995)
24.	Electronic Communications Security (Pty) Ltd Act, 2002 (Act 62 of 2002)
25.	General Intelligence Law Amendment Act, 2000 (Act 66 of 2000)
26.	Intelligence Service Act, 2002 (Act 65 of 2002) and regulations
27.	National Strategic Intelligence Act, 1994 (Act 39 of 1994)
28.	Intelligence Service Control Act, 1994 (Act 40 of 1994)
29.	Fire-arms Control Act, 2000 (Act 60 of 2000) and regulations
30.	Employment Equity Act, 1998 (Act 55 of 1998)
31.	National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
32.	Employment of Educators Act (EEA) (Act 76 of 1998)
33.	National Education Policy Act (Act 27 of 1996)
34.	Compensation for Occupational Injuries and Diseases Act (Act 181 of 1993)
35.	South African Schools Act (Act 84 of 1996)

36.	Western Cape Provincial School Education Act (No.12 of 1997)
37.	Protection of Administrative Justice Act, 2000 (Act 3 of 2000)

OTHER REGULATORY FRAMEWORK DOCUMENTS
Minimum Information Security Standards (MISS)
SACSA/090/1(4) Communication Security in the RSA
NIA Guidance Document: ICT Policy and Standards: Parts 1 & 2
ISO 17799
Government Gazette 2274,2001: Notice 1040
National Crime Prevention Strategy, 1996