LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
AGRICULTURE AND RURAL DEVELOPMENT

Security Policy

Ref: 2/5/P

Date of approval: 5 October 2016

Recommended by:

.....

Head of Department

(Maisela, RJ)

30/09/16

Date

Approved by:

.....

Honourable Member of Executive Council

Mapula Mokaba-Phukwana (MPL)

05/10/16

Date

Table of contents

1. Acronyms and abbreviations

BCP	Business Continuity Plan
COSMEC	Electronic Communications Security
HOD	Head of Department
ICT	Information and Communication Technology
IT	Information Technology
LDARD	Limpopo Department of Agriculture and Rural Development
MEC	Member of Executive Committee
SSA	State Security Agency
TSCM	Technical Surveillance Countermeasures
TRA	Threat and Risk Assessment

2. Executive summary

The Security Policy of the LDARD aims to address all matters regarding security within the Department. It provides detailed information on matters such as IT security, Communication security, the security manager, personnel security, physical security, the Security Committee and enforcement.

A detailed list of definitions as well as a detailed list of legislation which is applicable, is included in the policy.

3. Introduction

The Department of Agriculture and Rural Development depends on its personnel, information and assets to deliver services that ensure the health, safety, security and economic wellbeing of South African citizens. It must therefore manage these resources with due diligence and take appropriate measures to protect them.

Threats that can cause harm to the Department of Agriculture and Rural Development, in 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 results of changes in the international environment.

4. Purpose and objectives

The Security policy of Department of Agriculture and Rural Development prescribes the application of security measures to reduce the risk of harm that can be caused to the institution 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 Agriculture and Rural 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.

The main objective of this policy therefore is to support the national interest and the Department of Agriculture and Rural Development business objectives by protecting employees, information and assets and assuring the continued delivery of services to South African citizens.

This policy complements other Department of Agriculture and Rural Development policies (occupational health and safety, official languages, information management, asset control, real property and financial resources).

5. Authority

The security Policy for the LDARD has been developed under the custodianship of the HOD and approved by the MEC for Agriculture and Rural Development.

6. Legal Framework

This policy is informed by and complies with applicable national legislation, national security policies and national security standards.
The list is as follows:

1) Constitution of the Republic of South Africa, 1996 (act 106 of 1996)
2) Protection of information act, 1982 (act no. 84 of 1982)
3) Promotion of access to information act, 2000 (act no. 2 of 2000)
4) Promotion of administration justice act, 2000 (act 3 of 2000)
5) Copyright act, 1978 (act no. 98 of 1978)
6) National archives of South Africa act, 1996 (act no 43 of 1996) and regulations
7) Public service act, 1994 (act no. 103 of 1994) and regulations
8) Occupational health and safety act, 1993 (act no. 85 of 1993)
9) Criminal procedures act, 1977 (act 51 of 1977), as amended
10) Private security industry regulations act, 2001(act 56 of 2001)
11) Control of access to public premise and vehicles act, 1985 (act 53 of 1985)
12) National key points act, 1980 (act 102 of 1980)
13) Trespass act, 1959 (act 6 of 1959)
14) Electronic communication and transaction act, 2002 (act 25 of 2002)
15) Electronic communications security (PTY) Ltd Act, 2002 (act 68 of 2002)
16) State information technology agency act, 1998 (act 88 of 1998)
17) Regulation of interception of communications and provision of communication –related information act, 2002 (act 70 of 2002)
18) General intelligence law amendment act, 2000 (act 66 of 2000)
19) Intelligence service act, 2002 (act 65 of 2002) and regulations
20) National strategic intelligence act, 1994 (act 39 of 1994)
21) Intelligence service control act, 1994 (act 40 of 1994)
22) Labour relations act, 1995 (act 66 of 1995)
23) Employment equity act, 1998 (act 55 of 1998)
24) Occupational health and safety act, 1993, (act 83 of 1993)
25) Fire-arms control act, 2000 (act 60 of 2000) and regulations
26) Non-proliferation of weapons of mass destruction act, 1993 (act 87 of 1993)
27) Protection of constitutional democracy against terrorism and related activities act, 2004 (act 33 of 2004)
28) National building regulations and building standards act, 1977 (act 103 of 1977)
29) Protected disclosure act, 2000 (act 26 of 2000)
30) Intimidation act, 1982 (act 72 of 1982)

31) Prevention and combating of corrupt activities act, 2004 (act 12 of 2004)
32) Public finance management act, 1999 (act 1 of 1999) and treasury regulations
33) Fire Brigade act 99 of 1987
34) Basic Conditions of Employment act 75 of 1997
35) Compensation for Occupational Injuries and Disease act 61 of 1997
36) Arms and Ammunition act 75 of 1969
37) Civil Protection act 67 of 1977
38) Skills Development act 97 of 1998
39) Justice of the Peace and Commissioners of Oaths act 16 of 1963

Other regulatory framework documents

a) Minimum Information Security Standards (MISS), second edition March 1998
b) Minimum Physical Security Standards
c) White Paper on Intelligence (1995)
d) SACSA / 090/1 (4) Communication Security in the RSA
e) SSA Guidance documents: ICT Policy and Standards: part 1 & 2
f) ISO 17799
g) National Building Regulations;

7. Scope of application

A) This policy applies to the following individuals and entities:

1) All employees of Limpopo Department of Agriculture and Rural Development
2) All contractors and consultants delivering services to Limpopo Department of Agriculture and Rural Development
3) Temporary employees of Limpopo Department of Agriculture and Rural Development
4) All information assets of Limpopo Department of Agriculture and Rural Development
5) All intellectual property of Limpopo Department of Agriculture and Rural Development
6) All fixed property that is owned or leased by Limpopo Department of Agriculture and Rural Development

B) The policy further covers the following seven elements of the security program of the Limpopo Department of Agriculture and Rural Development:

1) Security organization
2) Security administration
3) Information security
4) Physical security
5) Personnel security

6) Information and Communication Technology (ICT) Security
7) Business Continuity Plan (BCP)

8. Definitions

"**Accreditation**" means the official authorization by management for the operation of an Information Technology (IT) systems, and acceptance by that management of the associated residual risk. Accreditation is based on the certificate process as well as other management considerations.

"**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 material, real property, financial resources, employee trust, public confidence and international reputation.

"**Availability**" means the condition of being usable on demand to support operations, programmes and services.

"**Business continuity planning**" includes the development of plans, measures, procedures and arrangements to ensure minimal or no interruptions 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 certifying that a comprehensive evaluation of the technical and non-technical security features of an Information and Communication Technology System (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.

"**COMSEC**" means the organ of state known as Electric Communications Security (PTY) LTD, which was established in terms of Section2 of the Electronic Communications Security Act,2002 (Act No. 68 of 2002).

"**Critical service**" means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which shall endanger the effective functioning of the institution.

"**Document**" means any note or writing, weather produced by hand or by printing, typewriting or any other similar process, in either tangible or electronic format, including:

- any copy, plan, picture, sketch or photographic or other representation of any place or article;
- any disk, 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:

a) document security;
b) physical security measures for the protection of information;
c) information and communication technology security;
d) personnel security;
e) business continuity planning;
f) contingency planning;
g) security scanning;
h) technical surveillance counter – measures;
I) dealing with information security breaches;
j) security investigations; and
k) administration and organization of the security function at organs of state.

"**National Intelligence Structure**" 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 thread materializing by exploitation of a vulnerability.

"**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.

"**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.

"**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 it is determined when to avoid, reduce and accept risk, as well as how to diminish the potential impact of a threatening event.

"**Vulnerably**" means a deficiency related to security that could permit to materialize.

9. Policy Pronouncements

9.1 General

1) Employees of Limpopo Department of Agriculture and Rural Development must be protected against identified threats according to baseline security requirements and continuous security risk management.

2) Information and assets of Limpopo Department of Agriculture and Rural Development must be protected according to baseline security requirements and continuous security risk management.

3) Continued delivery of services of Limpopo Department of Agriculture and Rural Development must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

9.2 Compliance requirements

9.2.1 Individuals

All individuals mentioned above must comply with the baseline requirements of this policy and it's associated Security Directives as contained in the Security Plan of Limpopo Department of Agriculture and Rural Development. These requirements are /shall be based on the integrated security Threat and Risk Assessment (TRA's) to the national interest as well as employees, information and assets of the Limpopo Department of Agriculture and Rural Development. The necessity of security measures above baseline levels shall also be determined by the continual updating of the security TRA's.

9.2.2 Security threat and risk assessment 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 LDARD 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 shall reduce the risk to an acceptable level.

9.2.3 Staff accountability and acceptable use of assets

The HOD of Limpopo Department of Agriculture and Rural Development shall ensure that information and assets of the Limpopo Department of Agriculture and Rural Development are used in accordance with procedures as stipulated in the Security Directives as contained in the Security Plan of the Limpopo Department of Agriculture and Rural Development.

All employees of Limpopo Department of Agriculture and Rural Development shall be accountable for the proper utilization and protection of such information and assets. Employees that misuse or abuse assets of Limpopo Department of Agriculture and Rural Development shall be held accountable therefore and disciplinary action shall be taken against any such employee.

9.3 Specific baseline requirements

9.3.1 Security organization

1) The HOD of Limpopo Department of Agriculture and Rural Development has appointed a Security Manager (DIRECTOR) to establish and direct a security program that ensures co-ordination of all policy functions and implementation of policy requirements.

2) Given the importance of this role, a DIRECTOR with sufficient security experience and training who is strategically positioned within the Limpopo Department of Agriculture and Rural Development so as to provide institution-wide strategic advice and guidance to senior management, has been appointed.

3) The HOD of Limpopo Department of Agriculture and Rural Development shall ensure that the DIRECTOR has an effective support structure (security component) to fulfil the functions referred to below.

4) Individuals that shall be appointed in the support structure of the DIRECTOR shall all be security professionals with sufficient security experience and training to effectively cope with their respective job functions.

i. Security administration

The functions referred to above include:

1) General security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets).
2) Setting of access limitations.
3) Administration of security screening.
4) Implementing physical security.
5) Ensuring the protection of employees.
6) Ensuring the protection of information.
7) Ensuring ICT security.
8) Ensuring security in emergency and increased threat situations.
9) Facilitating business continuity planning.
10) Ensuring security in contracting; and
11) Facilitating security breach reporting and investigation.

ii. Security incident / breaches reporting process

a) Whenever an employee of Limpopo Department of Agriculture and Rural Development 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 DIRECTOR of Limpopo Department of Agriculture and Rural Development by utilizing the formal reporting procedure prescribed in the Security breach directive of Limpopo Department of Agriculture and Rural Development.

b) The HOD of Limpopo Department of Agriculture and Rural Development shall report to the appropriate authority as indicated in the Security Breach Directive of Limpopo Department of Agriculture and Rural Development all cases or suspected cases of security breaches, for investigation.

c) The DIRECTOR of Limpopo Department of Agriculture and Rural Development shall ensure that all employees are informed about the procedure for reporting security breaches.

iii. Security incident / breaches response process

a) The DIRECTOR shall develop and implement a security breach response mechanism for Limpopo Department of Agriculture and Rural Development in order to address all security breaches / alleged breaches which are reported.

b) The DIRECTOR shall ensure that the HOD of Limpopo Department of Agriculture and Rural Development is advised of such incidents as soon as possible.

c) It shall be the responsibility of the State Security Agency and South African Police Services structures to conduct an investigation on reported security breaches and provide feedback with

recommendations to the Limpopo Department of Agriculture and Rural Development.

d) Access privileges to classified information, assets and / or to premises may be suspended by the HOD of Limpopo Department of Agriculture and Rural Development until administrative, disciplinary and / or criminal processes have been concluded, flowing from investigations into security breaches or alleged security breaches.

e) The end results of these investigations / disciplinary action or criminal prosecutions may be taken into consideration by the HOD of Limpopo Department of Agriculture and Rural Development 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.

iv. Information security

a) Categorization of information and information classification system:

b) The DIRECTOR must ensure that a comprehensive information classification system is developed for and implemented in Limpopo Department of Agriculture and Rural Development. All sensitive information produced or processed by Limpopo Department of Agriculture and Rural Development must be identified, categorized and classified according to the origin of its source and contents and according to its sensitivity to loss or disclosure.

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

1) State secret;
2) Trade secret;
3) Personal information.

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

(i) Confidential;
(ii) Secret;
(iii) Top secret.

d) Employees of Limpopo Department of Agriculture and Rural Development who generate sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labelling of classified documents.

e) 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.

f)Access to classified information shall be determined by the following principles:

(I) Intrinsic secrecy approach;
(II) Need to-know;
(III) Level of security clearance.

v. Physical Security

a) Physical security involves the proper layout and design of facilities of Limpopo Department of Agriculture and Rural Development and the use of physical security measures to delay and prevent unauthorized access to assets of Limpopo Department of Agriculture and Rural Development. It includes measures to detect and 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 and implemented in order to ensure that the entire Limpopo Department of Agriculture and Rural Development, its personnel, property and information are secured. These security measures must be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the DIRECTOR.

c)The Limpopo Department of Agriculture and Rural Development shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities. The Limpopo Department of Agriculture and Rural Development shall:

1) Select, design and modify facilities in order to facilitate the effective control of access thereto.
2) Demarcate restricted access areas and have the necessary entry barriers, security systems and equipment to effective control access thereto.
3) Include the necessary security specifications in planning, request for proposals and tender documentation.
4) Incorporate related costs in funding requirements for the implementation of the above.

d)Limpopo Department of Agriculture and Rural Development shall also ensure the implementation of appropriate physical security measures for the secure storage, transmission and disposal of classified and protected information in all forms.

9.3.2 Personnel Security

9.3.2.1 Security Screening

All employees, contractors and consultants of Limpopo Department of Agriculture and Rural Development, who requires access to classified information and critical assets in order to perform his / her duties or functions, must be subjected to a security screening investigation conducted by the State Security Agency (SSA) in order to be granted a security clearance at the appropriate level.

The level of security clearances 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.

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

A declaration of secrecy shall be signed by every individual issued with a security clearance to complement the entire security screening process. This shall remain valid even after the individual has terminated his / her services with Limpopo Department of Agriculture and Rural Development.

A security clearance shall 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 HOD of Limpopo Department of Agriculture and Rural Development, based on information which impact negatively on an individual's security competence.

Security clearance in respect of all individuals who have terminated their services with Limpopo Department of Agriculture and Rural Development shall be immediately withdrawn.

9.3.2.2 Polygraph examination

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.

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 shall not be granted.

9.3.2.3 Transferability of security clearances

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

9.3.2.4 Security awareness and training

The development and implementation of a security training and awareness program is the responsibility of the DIRECTOR. Effectively implementation ensure that all personnel and service providers of Limpopo Department of Agriculture and Rural Development remain security conscious.

All employees shall be subjected to the security awareness and training programs and must certify that the contents of the program(s) has been understood and shall be complied with. The program must 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 Limpopo Department

of Agriculture and Rural Development and the need to protect sensitive information against disclosure, loss or destruction.

Periodic security awareness presentations, briefings and workshops shall 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.

Regular surveys and walkthrough inspections shall be conducted by the DIRECTOR and members of the security component to monitor the effectiveness of the security training and awareness program.

9.3.2.5 IT Security

A secure network shall be established for Limpopo Department of Agriculture and Rural Development 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.

To prevent the compromise of IT systems, Limpopo Department of Agriculture and Rural Development 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.

To ensure policy compliance, the IT Manager of Limpopo Department of Agriculture and Rural Development shall:

a) Certify that all IT systems are secure after procurement, accredit IT systems prior to operation and comply with Minimum Security Standards and directive.

b) Conduct periodic security evaluations of systems, including assessment of configuration changes conducted on a routine basis.

c) Periodically request assistance, review and audits from the State Security Agency (SSA) in order to get an independent assessments.

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.

Access to the resources on the network of Limpopo Department of Agriculture and Rural Development shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of Limpopo Department of Agriculture and Rural Development shall be restricted unless explicitly authorized.

Systems hardware, operating and application software, the network and communication systems of Limpopo Department of Agriculture and Rural Development shall all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

All employees shall make use of IT systems of Limpopo Department of Agriculture and Rural Development in an acceptable manner and for business purposes only. All employees shall comply with the IT security directives in this regard at all times.

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.

To ensure the ongoing availability of critical services, Limpopo Department of Agriculture and Rural Development shall develop IT continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.

9.3.2.6 Internet access

The IT Manager of Limpopo Department of Agriculture and Rural Development, having the overall responsibility of setting up Internet access for Limpopo Department of Agriculture, shall ensure that the network of Limpopo Department of Agriculture and Rural Development is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. During induction and workshops. Human Resource Management shall ensure that all personnel with Internet access (including e-mail) are aware of, and shall comply with, an acceptable code of conduct in their usage of the internet.

The IT Manager of Limpopo Department of Agriculture and Rural Development shall be responsible for controlling user access to the internet, as well as for ensuring that

users are aware of the threats, and trained in the safeguards, to reduce the risk of information security breaches and incidents.

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.

9.3.2.7 Use of laptop computers

Usage of laptop computers by employees of Limpopo Department of Agriculture and Rural Development 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.

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

Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop computers at all times, in line with protection measures prescribed in the IT Security Directive.

9.3.2.8 Communication security

The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of Limpopo Department of Agriculture and Rural Development in all its forms and at all times.

All sensitive electronic communications by contractors or employees of Limpopo Department of Agriculture must be encrypted in accordance with the South African Communication Security Directive. Encryption devices shall only be purchased from SACSA or COMSEC and shall not be purchased from commercial suppliers.

Access to communication security equipment of Limpopo Department of Agriculture and Rural Development and the handling of information transmitted and / or received by such equipment, shall be restricted to authorized personnel only (personnel with a

proper Security Clearance who successfully completed the Communication Security Course).

9.3.2.9 Technical surveillance counter measures (TSCM)

All offices, meeting, conference and boardroom venues of Limpopo Department of Agriculture and Rural Development where sensitive and classified matters are discussed on 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) shall be conducted by SSA to ensure that these areas are kept sterile and secure.

The DIRECTOR of Limpopo Department of Agriculture and Rural Development 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.

No unauthorized electronic devices shall be allowed in any boardroom and conference facilities where sensitive information of Limpopo Department of Agriculture and Rural Development is discussed. Authorization must be obtained from the DIRECTOR.

9.3.2.10 Business Continuity Planning (BCP)

The DIRECTOR of Limpopo Department of Agriculture and Rural 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 employees, contractors, consultants and visitors.

The BCP shall be periodically tested to ensure that the management and employees of Limpopo Department of Agriculture understand how it is to be executed.

All employees of Limpopo Department of Agriculture and Rural Development shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.

The business continuity plan shall be kept up to date and re-tested periodically by the DIRECTOR.

9.4. SPECIFIC RESPONSIBILITIES

9.4.1 Head of institution

The HOD of Limpopo Department of Agriculture and Rural Development bears the overall responsibility for implementing and enforcing the security program of Limpopo Department of Agriculture and Rural Development. Towards the execution of this responsibility, the HOD shall:

a) Establish the post of the DIRECTOR 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 core business functions of Limpopo Department of Agriculture and Rural Development in the activities of the committee.

c) Approve and ensure compliance with this policy and its associated security directives which are applicable to the Department.

9.4.2 Security manager

The delegated security responsibility lies with the DIRECTOR of Limpopo Department of Agriculture and Rural Development who shall be responsible for the execution of the entire security function and program within Limpopo Department of Agriculture and Rural Development (coordination, planning, implementing, controlling, etc.) towards execution of his /her duties/ responsibilities, the DIRECTOR shall, amongst others:

a) chair the security committee of Limpopo Department of Agriculture and Rural Development;

b) draft the internal security policy and security plan (containing the specific and detailed security directives) of Limpopo Department of Agriculture and Rural Development in conjunction with the security committee;

c) review the security policy and security plan at regular intervals;

d) conduct a security TRA of Limpopo Department of Agriculture and Rural Development with the assistance of the security committee;

e) advise management on the security implications of management decisions;

f) implement a security awareness program;

g) conduct internal compliance audits and inspections at Limpopo Department of Agriculture and Rural Development at regular intervals;

h) establish a good working relationship with both SSA and SAPS and liaise with these institutions on a regular basis.

9.5 SECURITY COMMITTEE

The security committee referred to above shall consist of Senior Management of Limpopo Department of Agriculture and Rural Development representing all the main business units of Limpopo Department of Agriculture and Rural Development.

The security committee of the Limpopo Department of Agriculture and Rural Development shall be responsible for, amongst others:

Assisting the DIRECTOR in the execution of all security related responsibilities at Limpopo Department of Agriculture and Rural 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.

9.6 LINE MANAGEMENT

All Deputy Directors of Limpopo Department of Agriculture and Rural Development shall ensure that their subordinates comply with this policy and the security directives as contained in the security plan of Limpopo Department of Agriculture and Rural Development.

Deputy Directors 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.

Employees, consultants, contractors and other service providers:

Every employee consultant, contractor and other service providers of Limpopo Department of Agriculture and Rural Development 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 Limpopo Department of Agriculture and Rural Development at all times.

9.7 AUDIENCE

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

9.8 ENFORCEMENT

The HOD of Limpopo Department of Agriculture and Rural Development and the appointed DIRECTOR are accountable for the enforcement of this policy.

All employees of Limpopo Department of Agriculture and Rural Development are required to 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 Limpopo Department of Agriculture and Rural Development.

Prescripts to ensure compliance to this policy and the security directives by all consultants, contractors or service providers of Limpopo Department of Agriculture and Rural Development 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.

9.9 EXCEPTIONS

Deviations from this policy and its associate's security directives shall 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 HOD of Limpopo Department of Agriculture and Rural Development (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).

9.10 OTHER CONSIDERATIONS

The following shall be taken into consideration when implementing this policy:

a) Occupational health and safety issues in the Limpopo Department of Agriculture and Rural Development.
b) Disaster management at Limpopo Department of Agriculture and Rural Development.
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).

9.11 COMMUNICATING THE POLICY

The DIRECTOR of Limpopo Department of Agriculture and Rural Development 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 Limpopo Department of Agriculture and Rural Development. The DIRECTOR shall further ensure that all security policy and directive prescriptions are enforced and complied with.

The DIRECTOR must ensure that a comprehensive security awareness program is developed and implemented within Limpopo Department of Agriculture and Rural Development to facilitate the above said communication. Communication of the policy by means of this program shall be conducted as follows:

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 Limpopo Department of Agriculture and Rural Development.

9.12 REVIEW AND UPDATE PROCESS

The DIRECTOR, assisted by the security committee of Limpopo Department of Agriculture and Rural Development, must ensure that this policy and its associated security directives is reviewed and updated on an annual basis. Amendments shall be made to the policy and directives as the need arise.

9.13 IMPLEMENTATION

The DIRECTOR of Limpopo Department of Agriculture and Rural 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 Limpopo Department of Agriculture and Rural Development).

Implementation of the policy and its associated security directives is the responsibility of each and every individual this policy is applicable to.

9.14 MONITORING AND COMPLIANCE

A) The DIRECTOR, with the assistance of the security component and security committee of Limpopo Department of Agriculture and Rural Development must ensure compliance with this policy and its associated security directives by means of conducting internal security audits and inspections on a frequent basis. The findings of said audits and inspections shall be reported to the HOD of Limpopo Department of Agriculture and Rural Development forthwith after completion thereof.

B)Disciplinary action:

Non-compliance with this policy and its associated security directives shall result in disciplinary action which may include, but are not limited to:

1) re-training;
2) verbal and written warnings;
3) termination of contracts in the case of contractors or consultants delivering a service to Limpopo Department of Agriculture and Rural Development;
4) suspension;
5) loss of Limpopo Department of Agriculture and Rural Development information and assets resources access privileges.

Any disciplinary action taken in terms of non-compliance with this policy and its associated directives shall be in accordance with the disciplinary code / directive of Limpopo Department of Agriculture and Rural Development.

10 Default

To deviate from this Security Policy is a violation of the policy and will not be accepted. Should any deviation from this policy be needed, it will only take place with the written permission from the HOD (after proper motivation in this regard could be stated.) *Also refer to 9.9 – Exceptions.*

11 Inception date

The inception date of the Security Policy, is the date of approval.

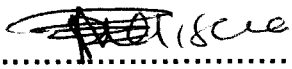
12 Termination and review

This policy on security within the LDARD, will be reviewed after 2 years (24 months) or as and when a need for review arise.

13 Enquiries

All enquiries regarding the Security Policy, should be directed towards Security Management at the LDARD at 015 294 3000 or Private Bag X 9487, POLOKWANE, 0700.

Recommended:

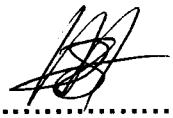


..... 2016-09-30

Maisela, RJ **Date**

(Head of Department)

Approved:



..... 05/10/16

Honourable Member of Executive Council **Date**

Mapula Mokaba-Phukwana (MPL)