

EASTERN CAPE PROVINCE



DEPARTMENT OF RURAL DEVELOPMENT AND AGRARIAN REFORM
SECURITY MANAGEMENT POLICY

TABLE OF CONTENTS

CHAPTER	PAGE
1. INTRODUCTION	3
2. PREAMBLE	3
3. PURPOSE	3
4. DEFINITIONS AND ABBREVIATIONS	4
5. SCOPE OF APPLICATION	7
6. LEGISLATIVE FRAMEWORK	8
7. GENERIC PRINCIPLES	10
8. ROLES AND RESPONSIBILITIES	17
9. COMMUNICATION AND DISTRIBUTION	20
10. ENFORCEMENT	21
11. AUDITING AND MONITORING	22
12. REVIEW AND UPDATE	22
13. REPORTING OF IRREGULARITIES AND/OR NON-COMPLIANCE	22
14. SANCTIONS FOR IRREGULARITIES AND/OR NON-COMPLIANCE	23
15. CONTACT DETAILS	23
16. APPENDICES	24

CHAPTER 1 INTRODUCTION

The Head of Department of Rural Development and Agrarian Reform (DRDAR) or his delegate with the assistance of the Security Committee has developed the DRDAR Security Policy in order to fulfill the security obligations of the DRDAR.

CHAPTER 2 PREAMBLE

This Security Policy is envisaged to regulate Information and Physical Security aspects and functions within DRDAR. This DRDAR Security Policy deals with the broader issues of security. In some parts of this DRDAR Security Policy, reference is made to its associated Security Directives. The Head of Department therefore has a responsibility for ensuring that such associated Security Directives are developed and form part of the Security Plan of the DRDAR.

CHAPTER 3 PURPOSE

This DRDAR Security Policy aims to regulate information Security aspects such as Document Security, Personnel Security, Information Communication Technology (ICT) Security, Technical Surveillance Counter Measures (TSCM), Business Continuity Planning, Contingency Planning, Vetting Investigation and Security Screening, dealing with information security Breaches, Security Investigations, Administration and organization of the Security function as well as Physical Security aspects within the DRDAR.

CHAPTER 4

DEFINITIONS AND ABBREVIATIONS

4.1 The following terms unless the context indicates otherwise:

- “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 interruption of the availability of critical services and assets;
- “critical service” means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the institution;
- “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 or Contingency Planning;
 - security screening;
 - technical surveillance countermeasures;
 - dealing with information security breaches;
 - security investigations; and
 - administration and organization of the security function at organs of state;
- “risk” means the likelihood of a threat materialising by exploitation of a vulnerability;
- “security breach” means the negligent or intentional transgression of or failure to comply with security measures;
- “Security Clearance” means an official document indicating the security competence of a person;
- “Security competence” means a person’s ability to act in such way that he/she does not cause classified information to fall into unauthorised hands thereby harming/jeopardising the security/interests of the State (it is measured against a person’s susceptibility to extortion/blackmail, amenability to bribes and susceptibility behaviour of compromise, loyalty to the State and relevant organ of state/institution);
- “Security Manager” means a person who ensures and manages information and physical security aspects and functions of the

Department;

- “security measures” means all actions, measures and means employed to achieve and ensure a condition of security commensurate with the prevailing threat.
- “South African Police Service” means the South African Police Service established by section 5(1) of the South African Police Service Act, 1995 (Act No 68 of 1995);
- “State Security Agency” means the Agency as defined in section 1 of the Intelligence Services Act, 2002 (Act 65 of 2002) as amended by the General Intelligence Laws Amendment Act, 2013 (Act No 11 of 2013);
- “service providers” means any close corporations, companies or any other business entities.
- “Technical Surveillance Countermeasures” (TSCM) means the process involved in the detection, localisation, identification and neutralisation of technical surveillance of an individual, an organ of state, facility or vehicle;
- “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; and
- “Vetting investigation” means the prescribed investigation followed in determining a person’s security competence.

4.2 The following abbreviations have the meaning allocated to them:-

- SAPS : South African Police Service
- SSA : State Security Agency
- TRA : Threat and Risk Assessment

CHAPTER 5

SCOPE OF APPLICATION

This DRDAR Security Policy applies to all employees of the DRDAR; all contractors and consultants delivering a service to the DRDAR, including their employees who may interact with the DRDAR; temporal employees of the DRDAR;

This DRDAR Security Policy further covers the following seven elements of the security program of the department:

- Security organization
- Security administration
- Information security
- Physical security
- Personnel security
- Information and Communication Technology (ICT) security
- Business Continuity Planning (BCP).

CHAPTER 6
LEGISLATIVE FRAMEWORK

6.1 This DRDAR Security Policy is informed by and complies with applicable legislation, provincial security policy, national security policies and National security standards.

6.2 The following legislation informs and regulates this DRDAR Security Policy:

- Constitution of the Republic of South Africa, 1996
- Control of Access to Public Premise and Vehicles Act, 1985 (Act No 53 of 1985)
- Copyright Act, 1978 (Act No 98 of 1978)
- Criminal Procedures Act, 1977, (Act No 51 of 1977)
- Electronic Communication and Transaction Act, 2002 (Act No 25 of 2002)
- Employment Equity Act, 1998 (Act No 55 of 1998)
- Firearms Control Act, 2000 (Act No 60 of 2000)
- Firearms Control Regulations, 2004
- Intimidation Act, 1982 (Act No 72 of 1982)
- Labour Relations Act, 1995 (Act No 66 of 1995)
- National Archives and Record Service of South Africa Act, 1996 (Act No 43 of 1996)
- National Archives and Record Service of South Africa Regulations, 2002,
- National Building Regulations and Building Standards Act, 1977 (Act No 103 of 1977)

- National Key Points Act, 1980 (Act No 102 of 1980)
- National Strategic Intelligence Act, 1994 (Act No 39 of 1994)
- Non-Proliferation of Weapons of Mass Destruction Act, 1993 (Act No 87 of 1993)
- Occupational Health and Safety Act, 1993 (Act No 85 of 1993)
- Prevention and Combating of Corrupt Activities Act, 2004 (Act No 12 of 2004)
- Private Security Industry Regulations Act, 2001 (Act No 56 of 2001)
- Promotion of Access to Information Act, 2000 (Act No 2 of 2000)
- Promotion of Administrative Justice Act, 2000 (Act No3 of 2000)
- Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act No 33 of 2004)
- Protected Disclosures Act, 2000 (Act No 26 of 2000)
- Protection of Information Act, 1982 (Act No 84 of 1982)
- Public Finance Management Act, 1999 (Act No 1 of 1999)
- Public Service Act, 1994 (Act No 103 of 1994)
- Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No 70 of 2002)
- State Information Technology Agency Act, 1998 (Act No 88 of 1998)
- Trespass Act, 1959 (Act No 6 of 1959)

6.3 Other regulatory framework documents

- Public Service Regulations, 2001
- International Organisation for Standardisation (ISO) 17799
- Minimum Information Security Standards (MISS), 1996
- Minimum Physical Security Standards (MPSS), 2009

CHAPTER 7
GENERIC PRINCIPLES:

7.1 Document Security

7.1.1 Classification and reclassification of documents:

7.1.1.1 Some units have at their disposal intelligence/information that is to some extent sensitive in nature and obviously requires security measures. The degree of sensitivity determines the level of protection, which implies that information must be graded or classified according to it. Every classification necessitates certain security measures with respect to the protection of sensitive information which will be known as classified information.

7.1.1.2 The responsibility for the gradings and regradings of document classifications rests with the institution where the documents have their origin. This function rests with the author or head of the institution or his/her delegate(s).

7.1.1.3 The classifications assigned to documents shall be strictly observed and may not be changed without the consent of the head of the institution or his delegate.

7.1.1.4 Where applicable, the author of a classified document shall indicate thereon whether it may be reclassified after a certain period or upon the occurrence of a particular event.

- 7.1.1.5 Should the author of a document on which there is no embargo, reclassify such document, he/she must inform all addressees of the new classification.
- 7.1.1.6 The receiver of a classified document who is of the opinion that the document concerned must be reclassified, must obtain oral or written authorisation from the author, the head of the institution or his delegate(s). Such authorisation must be indicated on the relevant document when it is reclassified.
- 7.1.1.7 The classification of a document or file will be determined by the highest-graded information it contains. The same classification as that of the original must be assigned to extracts from classified documents, unless the author consents to a lower classification.
- 7.1.1.8 Every document must be classified on its own merit (in accordance with its own contents) and in accordance with the origin of its contents, and not in accordance with its connection with or reference to some other classified document; provided that where the mere existence of a document referred to is in itself information that calls for a **higher** security classification than the document containing the reference, the **latter document** must be classified accordingly.
- 7.1.1.9 The author of a document must guard against the underclassification, overclassification or unnecessary classification of documents. The head of an institution or his/her delegate must on a regular basis test classifications of documents generated in his/her institution against the criteria applicable to the relevant classification.

7.1.1.10 Documents classified as Confidential should be stored in a reinforced steel filing cabinet.

7.1.1.11 Documents classified as Secret should be stored in a safe and/or strong room.

7.1.1.12 Documents classified as Top Secret should be stored in a safe and/or strong room.

7.1.1.13 Access to classified material/documents should be controlled and determined by the level of clearance one has obtained.

7.1.1.14 The destruction of classified documents shall be conducted according to the Archives Act of 1962.

7.1.1.15 The contingency plan of a department must provide for the destruction, storage and/or moving of classified/sensitive documents in the event of an emergency in order to prevent the risk of being compromised.

7.2 Personnel Security (Vetting Investigation and Security Screening):

All persons (applicants and employees) who will have access to classified information and intelligence in the possession of the DRDAR must undergo a vetting investigation conducted by the SSA in order to determine the security competence of persons (applicants and employees) and security screening to determine whether the service provider can be utilised.

7.2.1 All the DRDAR employees shall complete "Declaration of Secrecy" forms.

7.3 Physical Security Measures for the Protection of Classified Information:

The Security Manager should ensure that the physical security measures for the protection of classified information complies with the SSA's standards and request assistance from the South African Police Services regarding other Physical Security Measures.

7.4 Physical security aspects

7.4.1 Access to the Office of the Premier buildings shall be controlled and monitored by security personnel.

7.4.2 Effective key control must be instituted. The keeping of the necessary key registers and the safe custody of duplicate keys and control over such keys must be strictly adhered to.

7.4.3 Measures to be put in place to enforce negligent loss of keys by personnel.

7.4.4 The Security Manager in conjunction with other relevant units (Facilities and Security Management, HR, Labour Relations) 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.

- 7.4.5 The BCP shall be periodically tested to ensure that the management and employees understand how it is to be executed.
- 7.4.6 All employees shall be made aware and trained on the content of the BCP to ensure understanding of their own respective roles in terms thereof.
- 7.4.7 The Business Continuity Plan shall be kept up to date and re-tested periodically by the Security Manager.
- 7.5 **Technical Surveillance Counter measures (TSCM):** The Senior Management should ensure that TSCM services (sweeps or inspections) are conducted by the SSA TSCM Technicians (in meetings where classified information will be discussed, occupancy of new office buildings/offices, occurrence of security breaches). The TSCM services (sweeps and inspections) may be procured at no costs from the SSA to detect and sterilise the venues against possible bugs and monitoring devices.
- 7.6 **Information and Communication Technology (ICT) Security:** ICT security in terms of section 2(b) of the National Strategic Intelligence Act, 1994 (Act No 39 of 1994) as amended by the General Intelligence Laws Amendment Act, 2013 (Act No 11 of 2013), the SSA provides cryptographic and verification services for electronic communications security systems, products and services used by organs of state; develops, designs, invents, procures, installs or maintains and coordinates research regarding electronic communications security systems, products and services.

7.6.1 A secure network shall be established for the DRDAR 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.

7.6.2 To prevent the compromise of ICT systems, the DRDAR 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.

7.6.3 To ensure policy compliance, departmental ICT Management shall:

- certify that all ICT systems are secured after procurement, accredit ICT 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 Agency (SSA) in order to get an independent assessment.

7.6.4 Server rooms and other related security zones where ICT equipment are kept shall be secured with adequate physical security measures and strict access control shall be enforced and monitored.

- 7.6.5 Access to the resources on the network of the DRDAR shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of the DRDAR shall be restricted unless explicitly authorized.
- 7.6.6 ICT System hardware, operating and application software, the network and communication systems of the DRDAR shall all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.
- 7.6.7 All employees shall make use of ICT systems of the DRDAR in an acceptable manner and for business purposes only. All employees shall comply with the ICT acceptable Security Directives in this regard at all times.
- 7.4.8 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.
- 7.4.9 To ensure the on-going availability of critical services, the DRDAR, shall develop ICT continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.

CHAPTER 8

ROLES AND RESPONSIBILITIES

8.1 Head of Institution

8.1.1 The Head of DRDAR bears the overall responsibility for implementing and enforcing the security program of DRDAR. Towards the execution of this responsibility, the Head of DRDAR, shall:-

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

8.2 Security Manager

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

- chair the security committee of DRDAR;

- draft the internal Security Policy and Security Plan (containing the specific and detailed Security Directives of DRDAR) in conjunction with the security committee;
- review the Security Policy and Security Plan at regular intervals;
- conduct a security TRA of DRDAR with the assistance of the security committee;
- advise management on the security implications of management decisions;
- implement a security awareness program;
- conduct internal compliance audits and inspections at DRDAR at regular intervals;
- establish a good working relationship with both SSA and SAPS and liaise with these institutions on a regular basis.
- supervise the implementation of physical security measures for the DRDAR
- ensure that SMS members and other specific officials (e.g. procurement), complete and submit their required security clearance forms.
- maintain a database of all security breaches cases reported and/or detected.

8.3 Security Committee

8.3.1 The Security Committee shall consist of senior managers representing all the main business units of the DRDAR.

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

8.3.3 The Security Committee of the DRDAR shall be responsible for, amongst others:-

- Assisting the Security Manager in the execution of all security related responsibilities at DRDAR, including completing tasks such as drafting/reviewing of the Security Policy and Plan, ensuring that the TRA is conducted, verifying and overseeing security audits, drafting of a BCP and assisting with security awareness and training.

8.4 Line Management

8.4.1 All managers of DRDAR shall ensure that subordinates comply with this policy and the Security Directives as contained in the Security Plan of DRDAR at all times.

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

8.5 Employees, Consultants, Contractors and other Service Providers

8.5.1 Every employee, consultant, contractor and other service providers of DRDAR shall know what their security responsibilities are, accept it as part of their normal job function, and not only co-operate, but contribute to improving and maintaining security at DRDAR at all times.

CHAPTER 9 COMMUNICATION AND DISTRIBUTION

9.1.1 The Security Manager of DRDAR shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees, consultants, contractors, service providers, clients, visitors and members of the public that may officially interact with the DRDAR. The Security Manager will further ensure that all security policy and directive prescriptions are enforced and complied with.

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

- Awareness workshops and briefings to be attended by all employees;
- Distribution of memos and circulars to all employees;
- Access to the policy and applicable directives on the intranet of DRDAR.

CHAPTER 10 ENFORCEMENT¹

10.1.1 The Head of DRDAR and the appointed Security Manager are accountable for the enforcement of this policy.

10.1.2 All employees of DRDAR 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 DRDAR.

10.1.3 Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contractors or service providers of DRDAR shall be included in the contracts signed with such individuals, institutions and / or 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 contract, depending on the nature of any non –compliance.

¹Indicate the responsible person who will ensure the enforcement of this SP.

CHAPTER11
AUDITING AND MONITORING

11.1.1 The Security Manager with the assistance of the security component and security Committee of DRDAR must ensure compliance with this Policy and its associated Security Directives by means of conducting internal security audits and inspections on a frequent basis.

11.1.2 The findings of said audits and inspections shall be reported to the Head of DRDAR forthwith after completion thereof.

CHAPTER 12
REVIEW AND UPDATE

12.1.1 The SM assisted by the Security Committee of DRDAR must ensure that this policy and its associated Security Directives is reviewed and updated once every Five (5) years. Amendments shall be made to the policy and directives as the need arise.

CHAPTER 13
REPORTING OF IRREGULARITIES AND/OR
NON-COMPLIANCE

13.1.1 Irregularities and/or non-compliance with Security Policy of the DRDAR must be reported to the SM within 24 hours of noticing the occurrence and can be reported in writing via, telephone or e-mail.

CHAPTER 14

SANCTIONS FOR IRREGULARITIES AND/OR NON-COMPLIANCE

14. Irregularities and/or non-compliance with this Security Policy by a member of the DRDAR may result in disciplinary procedures and/or sanctions which may include, but not limited to:
- Verbal and written warnings;
 - Termination of contracts in the case of contractors or consultants delivering services to the DRDAR;
 - Dismissal;
 - Suspension and
 - Withdrawal of access to information and resources of the DRDAR.
- 14.2 Any disciplinary action taken against non-compliance with this policy and its associated directives will be in accordance with the disciplinary code/directives of the DRDAR.

CHAPTER 15

CONTACT DETAILS²

- 15.1.1 Members of the DRDAR should address queries regarding the content, interpretation and application of this Security Policy to the office of Manager, Security Management Services.

² Indicate the responsible person who will serve as a nodal point to address queries regarding the content, interpretation and application of this SP.

17. RECOMMENDATION/ NOT RECOMMENDED

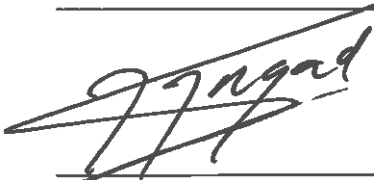
Comments: This Policy provide a guide on
how to manage security related issues



CHEF OPERATIONS OFFICER DATE: 27/03/18

APPROVED / ~~NOT APPROVED~~

Comments: _____



HEAD OF DEPARTMENT: DRDAR DATE: 28/03/2018