PROVINCE OF THE EASTERN CAPE

DEPARTMENT OF RURAL DEVELOPMENT

AND

AGRARIAN REFORM

ARCHIVES AND RECORD MANAGEMENT POLICY

Table of Contents

DEFINITION OF TERMS AND CONCEPTS

Archives repository: The building in which records with archival value are preserved permanently.

Authentic records: Authentic records are records that can be proven to be what they purport to be. They are also records that are considered by the creators to be their official record.

Authoritative records: Authoritative records are records that are authentic, reliable, trustworthy, and useable and are complete and unaltered.

Correspondence system: A set of paper-based and electronic communications and associated documents, sent, received, generated, processed, and stored during the conduct of business.

Custody: The control of records based upon their physical possession.

Disposal: The action of either destroying/deleting a record or transferring it into archival custody.

Disposal authority: A written authority issued by the National Archivist specifying which records should be transferred into archival custody or specifying which records should be destroyed/deleted or otherwise disposed of.

Disposal authority number: A unique number identifying each disposal authority issued to a specific office.

Electronic records: Information which is generated electronically and stored by means of computer technology. Electronic records can consist of an electronic correspondence system and electronic record systems other than the correspondence system.

Electronic records system: This is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and meta data (background and technical information i.t.o. the information stored electronically) and in hard copy. All these components are defined as records by the

	Act. They must therefore be dealt with in accordance with the Act's provisions.
File plan:	A pre-determined classification plan by which records are filed and/or electronically indexed to facilitate efficient retrieval and disposal of records.
Filing system:	The collective noun for a storage system (like files, boxes, shelves or electronic applications and storage systems) in which records are stored in a systematic manner according to a file plan.
Non-archival records:	Records with a short-lived interest or usefulness.
Public record:	A record created or received by a governmental body in pursuance of its activities, regardless of form or medium.
Records other than correspondence systems:	Records that do not form part of a correspondence file, or a case file e.g. registers, maps, plans, electronic records, audio-visual records, etc.
Record:	Recorded information regardless of form or medium.
	Evidence of a transaction, preserved for the evidential information it contains.
Records classification system:	A plan for the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in the classification system.
Recording:	Anything on which sounds or images or both are fixed or from which sounds or images or both are capable of being reproduced, regardless of form.
Record keeping:	Making and maintaining complete, accurate and reliable evidence of official business in the form of recorded information.
Records management:	Records management is a process of ensuring the proper creation, maintenance, use and disposal of records throughout their life cycle to achieve efficient, transparent and accountable governance.

Retention period:	The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.
Data Subject:	person to whom personal information relates
Responsibility Party:	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
Right of Appeal:	a responsible party on whom an information or enforcement notice has been served, within 30 days of receiving the notice, appeal to the high court, having jurisdiction for the setting aside or variation of the notice.
Information Officer:	means the Head of Department/ Accounting Officer of the Department
Deputy Information Officer:	means an official of the Department appointed by the HOD (Deputy Director: Records Management) in terms of PAIA and POPIA
Lawful Processing of Personal Information:	means collection of personal information must be for specifically defined, lawful purpose related to a function of the responsible party and consent must be obtained.
Biometrics:	means a technique of personal identification that is based on physical, psychological, or behavioral characteristics including blood typing, fingerprints, DNA analysis, retinal and voice recognition.

Schedule for records other than correspondence systems:

A control mechanism for records other than correspondence files (other records), which contains a description and the disposal instructions and retention periods of all other records. It consists of the following parts:

- Schedule for paper-based records other than correspondence files.
- Schedule for electronic records systems other than the electronic correspondence system.
- Schedule for microfilm records.
- Schedule for audio-visual records.

System technical manual: A manual containing information regarding the hardware, software and network elements that comprise the system and how they interact. Details of all changes to a system should also be documented.

System procedures manual: A manual containing all procedures relating to the operation and use of the electronic system, including input to, operation of and output from the system. A system procedures manual would contain detailed procedures regarding -

- Document capture
- Document scanning
- Data capture
- Indexing
- Authenticated output procedures
- File transmission
- Information retention
- Information destruction
- Backup and system recovery
- System maintenance
- Security and protection
- Use of contracted services
- Workflow
- Date and time stamps
- Version control
- Maintenance of documentation

A systems procedures manual should be updated when new releases force new procedures.

1. INTRODUCTION

Section 13 of the National Archives and Records Service of South Africa Act No 43 of 1996 and Provincial Archives and Records Services Act No 7 of 2003; require the Department to manage its records in a well-structured record keeping system. The Department puts the necessary policies and procedures in place to ensure that its record keeping, and management practices comply with the requirements of the Act.

The Department has realized that vital information of the Department at times cannot be traced and end up being lost forever. Loss of any vital departmental information/records can put the Department in an awkward position and should such information lend in the wrong hands the individual's privacy and image of the Department can be compromised. Some of the records that the Department ought to keep and manage include classified personal information of staff and other classified information. There is a standardized procedure for classification of documents, recording, storage/archiving and set timeframes by which records can be disposed. Therefore, through this policy the Department is trying to enforce archive and record management systems that should be adhered to by all employees of the Department and responsible officials at head office, district offices, local offices and institutions of the Department. This is the background against which this policy is developed.

2. REGULATORY FRAMEWORK

By managing its paper-based records effectively and efficiently the Department strives to give effect to the accountability, transparency and service delivery values contained in the legal framework established by:

- 2.1. Constitution of the Republic of South Africa Act No. 108 of 1996.
- 2.2. National Archives and Records Service of South Africa Act No.43 of 1996 as amended.
- 2.3. Provincial Archives and Records Services Act No.7 of 2003).
- 2.4. National Archives and Records Service of South Africa Regulations.
- 2.5. Public Finance Management Act No.1 of 1999; (PFMA).
- 2.6. Promotion of Access to Information Act No. 2 of 2000; (PAIA).
- 2.7. Promotion of Administrative Justice Act No.3 of 2000; (PAJA).
- 2.8. Protection of Personal Information Act No. 4 of 2013 (POPIA).
- 2.9. Electronic Communications and Transactions Act No. 25 of 2002.
- 2.10. Security Management Policy of DRDAR as approved.
- 2.11. Minimum Information Security Standards (MISS)

3. OBJECTIVES

The objectives of this policy are to:

- 3.1. enable the Department to find the right information easily and comprehensively.
- 3.2. enable the Department to perform its functions and conduct its business in an orderly, successfully, efficient, and accountable manner.
- 3.3. support the business, legal and accountability requirements of the Department.

3.4. ensure the consistent delivery of services.
3.5. support and document policy formation and administrative decision-making.
3.6. provide continuity in the event of a disaster.
3.7. protect the interests of the Department and the rights of employees, clients, and present and future stakeholders.
3.8. support and document the Department's activities, development, and achievements.
3.9. Promote knowledge management and institutional memory.
3.10. Give effect to the Constitutional Right to privacy, by safeguarding personal information.
3.11. Regulate the manner in which personal information may be processed.

4. PRINCIPLES, VALUES AND PHILOSOPHY

All records created and received by the Department are managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act, 1996 and Provincial Archives and Records Services Act No. 7 of 2003.

The following broad principles apply to the record keeping and management practices of the Department:

4.1. Following sound procedures for the creation, maintenance, retention, and disposal of all records.
4.2. Ensuring that the records management procedures of the Department comply with legal requirements, including those for the provision of evidence.
4.3. Ensuring sound procedures for the security, privacy, and confidentiality of its records.
4.4. Electronic records are managed according to the principles promoted by the National Archives and Records Service.
4.5. Ensuring that the Department has performance measures for all records management functions and reviews compliant with these measures.

5. SCOPE OF APPLICABILITY

5.1. This policy covers the department's work practices for all those who:
5.1.1. Create records including electronic records.
5.1.2. Have access to records.
5.1.3. Have any other responsibilities for records, for example storage and maintenance responsibilities.
5.1.4. Have management responsibility for staff engaged in any of these activities; or manage or have design input into information technology infrastructure.
5.2. The policy therefore applies to all staff members of the Department and covers all records regardless of format, medium or age.

6. IMPLEMENTATION PROCEDURES

6.1. Records classification systems and related storage areas. The Department has the following systems that organize and store records:

Correspondence systems

6.1.1. Departmental File plan

6.1.2. Only the File Plan approved on 04 December 2013 shall be used for the classification of correspondence records. The file plan shall be used for the classification of paper-based records.

6.1.3. Each staff member shall allocate file reference numbers to all correspondence (paper) according to the approved subjects in the file plan.

6.1.4. When correspondence is created /received for which no subject exists in the file plan, the records manager should be contacted to assist with additions to the file plan. Under no circumstances may subjects be added to the file plan if they have not been approved by the records manager.

6.2. Storage areas

6.2.1. Paper-based correspondence files are kept in the custody of-

6.2.1.1. The Main Registry

6.2.1.2. All paper-based correspondence system records that are not HR related are housed in the Main Registry.

6.2.1.3. All these records are under the management of the records manager who is mandated to ensure that they are managed properly.

6.2.1.4. The registry is a secure storage area and only registry staff is allowed in the records storage area.

6.2.1.5. Staff members who need access to files in the registry shall place a request for the files at the counter.

6.2.1.6. The registry shall be locked when registry is not in operation, and when the staff is sorting departmental mail.

6.3. The Human Resources Registry

6.3.1. All Human Resources related records are housed in the HR Registry.

6.3.2. The general HR subject files as well as HR case files are under the management of the records manager who is mandated to ensure that they are managed properly.

6.3.3. The Department maintains a set of paper-based case files for each staff member. These files are confidential in nature and are housed in a secure storage area in the HR registry.

6.3.4. The case files are managed as part of the List of Series of Separate Case Files that is maintained and managed by the records manager.

6.3.5. The files exist only in paper-based format and the physical tracking of the case files are managed with the file tracking system in the Integrated Document and Records Management System.

6.4. **Electronic correspondence records**

6.4.1. These records will be stored in an electronic repository that will be maintained by the IT section in conjunction with the records manager.

6.4.2. Access to storage areas where electronic records are stored will be limited to the Records Manager and the Information Technology staff who have specific duties regarding the maintenance of the hardware, software and media.

6.5. **Records other than correspondence systems**

6.5.1. Schedule for records other than correspondence systems.

6.5.2. The Records Manager maintains a schedule of all records other than the correspondence system. The schedule contains a description of each set of records other than the correspondence system and indicates the storage location and retention periods of these records regardless of format.

6.6. **Storage areas**

6.6.1. Paper-based

a) The Department has sets of paper-based records other than the correspondence systems that are in the custody of the various officials that use them on a daily basis.

b) These records are under the control of the records manager who is mandated to ensure that they are managed properly.

6.7. **Audio-visual records**

6.7.1. The Department must have sets of audio-visual records that are stored safely and properly.

6.7.2. These records are under the control of the records manager who is mandated to ensure that they are managed properly.

6.8. Electronic systems other than the correspondence systems

6.8.1. The Records Manager must oversee electronic systems such as video recordings of departmental events, record tapes of departmental meeting and hearings.

6.8.2. The IT manager is responsible for the maintenance of these systems.

6.8.3. The records maintained in these systems are under the control of the records manager who is mandated to ensure that they are managed properly.

6.9. **Disposal of Records**

6.9.1. No public records (including e-mail) shall be destroyed, erased or otherwise disposed of without prior request from records manager who in turn shall seek written authorization from the Accounting Officer.

6.9.2. Retention periods indicated on the filing system must be determined by taking the Department's legal obligations and functional needs into account. Should a staff member disagree with the allocated retention periods, the records manager should be contacted to discuss a more appropriate retention period.

6.9.3. Disposal in terms of disposal authorities issued by Provincial Archives must be executed once a year.

6.9.4. All disposal actions should be authorized by the records manager prior to their execution to ensure that archival records are not destroyed unintentionally.

6.9.5. Non-archival records that are needed for litigation, Promotion of Access to Information requests or Promotion of Administrative Justice actions must not be destroyed until such time that the Manager: Legal Services has indicated that the destruction hold can be lifted.

6.9.6. Paper-based archival records must be safely kept in an off-site storage facility until they are due for transfer to the Provincial Archives Repository. Transfer procedures must be as prescribed by the Provincial Archives in the *Records Management Policy Manual.*

6.10. **Storage and custody**

6.10.1. All records must be kept in storage areas that are appropriate for the type of medium. The Provincial Archives and Records Services' guidelines contained in the *Records Management Policy Manual* must apply.

6.11. **Access and security**

6.11.1. Records must at all times be protected against unauthorized access and tampering to protect their authenticity and reliability as evidence of the business transactions of the Department.

6.11.2. Security of classified records must be managed in terms of the Security Management Policy which will be available from the Office of the Head of Department.

6.11.3. No staff member must remove records that are not available in the public domain from the premises of the Department without the explicit permission of the Head of the Department.

6.11.4. No staff member must provide information and records that are not in the public domain to the public without consulting the records manager. Specific guidelines regarding requests for information are contained in the Promotion of Access to Information Act.

6.11.5. Personal information must be managed in terms of the Promotion of Access to Information Act.

6.11.6. No staff member must disclose personal information of any member of staff or client of the Department to any member of the public without consulting the records manager first.

6.11.7. Records storage areas must at all times be protected against unauthorized access.

6.11.8. Registry and other records storage areas must be locked when not in use.

6.11.9. Special Personal Information relates to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information.

6.12. **Legal admissibility and evidential weight**

The records of the Department must at all times contain reliable evidence of business operations. The following shall apply:

6.13. **No records must be removed from paper-based files without the explicit permission of the records manager.**

6.13.1. Records that were placed on files must not be altered in any way.

6.13.2. No alterations of any kind must be made to records other than correspondence files without the explicit permission of the records manager.

6.13.3. Should evidence be obtained of tampering with records, the staff member involved must be subject to disciplinary action.

6.14. **Electronic records**

6.14.1. The Department shall use systems which ensure that its electronic records are:

a) Authentic
b) not altered or tampered with
c) auditable; and
d) Produced in systems which utilize security measures to ensure their integrity.

6.15. **Training**

6.15.1. The Records Manager must successfully complete the Archives and Records Service's Records Management Course, as well as any other Records Management training that would equip him/her for his/her duties.

6.15.2. The Records Manager must identify such training courses that are relevant to the duties of the registry staff and must ensure that the registry staff is trained appropriately.

6.15.3. The Records Manager must ensure that all staff members are aware of the Records Management Policies and must conduct or arrange such training as is necessary for the staff to equip them for their records management duties.

7. ROLES AND RESPONSIBILITIES

7.1. Head of the Department

7.1.1. The Accounting Officer (Information Officer) is ultimately accountable for the record keeping and records management practices of the Department.

7.1.2. The Accounting Officer is committed to enhance accountability, transparency and improvement of service delivery by ensuring that sound records management practices are implemented and maintained.

7.1.3. The Accounting Officer supports the implementation of this policy and requires each staff member to support the values underlying in this policy.

7.1.4. The Accounting Officer must designate a Deputy Director to be the Records Manager of the Department and must mandate the records manager to perform such duties as are necessary to enhance the record keeping and records management practices of the Department to enable compliance with legislative and regulatory requirements.

7.2. **Senior Management Services (SMS)**

7.2.1. SMS is responsible for the implementation of this policy in their respective units.

7.2.2. Must lead by example and shall themselves maintain good record keeping and records management practices.

7.2.3. Ensure that all staff is made aware of their record keeping and records management responsibilities and obligations.

7.2.4. Must ensure that the management of records including e-mail is a key responsibility in the performance agreements of all the staff in their units and managed as per the departmental ICT policy.

7.3. **Records Manager**

The Records Manager is responsible for:

7.3.1. The implementation of this policy.

7.3.2. Staff awareness regarding this policy.

7.3.3. The management of all records according to the records management principles contained in the National Archives and Records Service Act 43, of 1996 and Provincial Archives and Records Services Act 7, of 2003.

7.3.4. The determination of retention periods in consultation with the users and considering the functional, legal, and historical need of the body to maintain records of transactions.

7.3.5. The Records Manager is mandated to make such training and other interventions as are necessary to ensure that the Head of the Department's record keeping, and records management practices comply with the records management principles contained in the Provincial Archives and Records Service Act 7 of 2003.

7.3.6. The Records Manager must from time-to-time issue circulars and instructions regarding the record keeping and records management practices of the Department.

7.3.7. The Records Manager must ensure that all records created and received by the Department are classified according to the approved file plan and that a written disposal authority is obtained for them from the Provincial Archives and Records Service.

7.3.8. The post designation is the Records Manager for the whole Department.

7.4. **IT Manager**

7.4.1. The IT manager is responsible for the maintenance of electronic systems that stores records.

7.4.2. The IT manager must work in conjunction with the Records Manager to ensure that public records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes.

7.4.3. The IT manager must ensure that appropriate *systems technical manuals* and *systems procedures manuals* are designed for each electronic system that manages and stores records.

7.4.4. The IT manager must ensure that all electronic systems capture appropriate systems generated metadata and audit trail data for all electronic records to ensure that authentic and reliable records are created.

7.4.5. The IT manager must ensure that electronic records in all electronic systems remains accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence.

7.4.6. The IT manager must ensure that all data, metadata, audit trail data, operating systems and application software are backed up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur.

7.4.7. The IT manager must ensure that back-ups are stored in a secure off-site environment.

7.4.8. The IT manager must ensure that systems that manage and store records are virus free.

7.5. Security Manager

7.5.1. The security manager must be responsible for the physical security of all records.

7.5.2. Must ensure that all Registry Staff is vetted.

7.6. Legal Services Manager

7.6.1. The Legal Services Manager must keep records manager updated about developments in the legal and statutory environment that may impact on the record keeping and records management practices of the Department.

7.7. Registry staff

7.7.1. The registry staff is responsible for the physical management of the records in their care.

7.7.2. Detailed responsibilities regarding the day-to-day management of the records in the registry are contained in the *Registry Standard Operating Procedures.*

7.8. Staff

7.8.1. Every staff member must create records of transactions while conducting official business.

7.8.2. Every staff member must manage those records efficiently and effectively by:

a) Allocating reference numbers and subjects to paper-based records according to the file plan.
b) Sending paper-based records to the registry for filing.
c) Ensuring that records are destroyed/deleted only in accordance with the written disposal authority obtained from the Records Manager.

7.8.3. Records management responsibilities must be written into the performance agreements of all staff members to ensure that staff is evaluated on their records management responsibilities.

8. RESOURCE IMPLICATIONS

The implementation and management of this policy requires financial and human resource support.

9. MONITORING

Records Manager must ensure Implementation, Monitoring and Evaluation of this policy as detailed in this policy framework and procedure manual.

10. POLICY REVIEW

This policy shall be reviewed after 5 years upon approval or when a need arises to ensure that it meets the business and service delivery requirements of the Department.

11. RECOMMENDATIONS & APPROVALS

Approved / ~~Not Approved~~

....

....

....

MR B. DAYIMANI
ACTING HEAD OF DEPARTMENT (DRDAR)
DATE: 28/03/2024