LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
TRANSPORT

RECORDS MANAGEMENT POLICY

VERSION 3

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

1. HR – Human Resources
2. IT – Information Technology
3. MEC – Member of Executive Council
4. MISS – Minimum Information Security Standards
5. NARSA – National Archives and Records Services Act
6. RM – Records Management

DEFINITIONS

A20 - Valuable records that should be transferred to an appropriate archives repository for permanent preservation **20 years** after the end of the year in which the record was closed

Appraisal - The decision regarding the preservation requirements of each document

Archives - A record already in the custody of an archives repository or records centre

Archival Value - This refers to the long term use records may have for purposes other than functional use. Also known as A20

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.

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

Disposal authority - A written authority issued by the National/Provincial 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.

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.

IT Manager Designated Officer

Non-archival records Records with a short lived interest or usefulness.

Public Records - 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 -

1) Recorded information regardless of form or medium.
2) 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.

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.

Records Manager - Designated Officer

Retention period - The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.

Records Control Schedule – This is an instrument to control records other than correspondence files according to which such items are identified and disposed.

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

Security Manager - Designated Officer

1. INTRODUCTION AND BACKGROUND

The Department is committed to promote noble constitutional values such as efficiency, transparency and accountability through sound records management. It is worth noting that sound records management is a central tenet of democratic governance features. Good record - keeping is also the cornerstone of any efficient, transparent and accountable administration. The value of a record in public administration cannot be emphasized because every administrative process or transaction conducted by a government official involves or is informed by a record. A single transaction has the potential to generate multiple documents either through creation or receipt.

This policy therefore, aims to address inconsistencies and uncertainties with regard to records management practice within the Department. It is aimed at encouraging uniformity in the execution of records management functions amongst institutions within the Department. The policy also provides the framework for the Department to effectively fulfil its obligations and statutory requirements under the archival legislation in the new dispensation.

2. PURPOSE AND OBJECTIVE

The purpose of the Records Management policy is to give a directive towards proper creation, receipt, care utilization and disposal of records when legal and administrative requirements have been satisfied in compliance to the prescripts.

3. LEGAL FRAMEWORK

3.1 Constitution of the Republic of South Africa, (Act No 108 of1996)

3.2 National Archives and Records Service of South Africa Act (Act No 43 of 1996 as amended)

3.3 National Archives and Records Service of South Africa Regulations (R126 of 1997)

3.4 Public Finance Management Act (Act No 1 of 1999)

3.5 Promotion of Access to Information Act (Act No 2 of 2000)

3.6 Promotion of Administrative Justice Act (Act No 3 of 2000)

3.7 Electronic Communications and Transactions Act (Act No 25 of 2002)

3.8 The Minimum Information Security Standard (MISS)

3.9 Provincial Archives Act.

4. POLICY STATEMENT

4.1 All records created and received by the Department shall be managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act, 1996.

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

4.2.1 The Department follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.

4.2.2 The records management procedures of the Department comply with legal requirements, including those for the provision of evidence.

4.2.3 The Department follows sound procedures for the security, privacy and confidentiality of its records.

4.2.4 Electronic records in the Department are managed according to the principles promoted by the National Archives and Records Service.

4.2.5 The Department has performance measures for all records management functions and reviews compliance with these measures.

5. POLICY PRONOUNCEMENT

5.1 This policy impacts upon Department 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. SCOPE OF APPLICATION

This policy applies to all employees of the Limpopo Department of Transport.

7. ROLES AND RESPONSIBILITIES

7.1 Head of Department

7.1.1 The Head of Department is ultimately accountable for the record keeping and records management practices of the Department.

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

7.1.2 The Head of Department supports the implementation of this policy and requires each staff member to support the values underlying in this policy.

7.1.3 The Head of Department shall designate a Director to be the Records Manager of the Department and shall 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 Chief Directors

7.2.1 Chief Directors are responsible for the implementation of this policy in their respective units.

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

7.2.3 Chief Directors shall ensure that all staff members are made aware of their record keeping and records management responsibilities and obligations.

7.3 Records Manager

7.3.1 The Records Manager is responsible for:

7.3.2 the implementation of this policy

7.3.3 staff awareness regarding this policy

7.3.4 the management of all records according to the records management principles contained in the National Archives and Records Service Act, 1997.

7.3.5 the determination of retention periods in consultation with the users and taking into account the functional, legal and historical need of the body to maintain records of transactions.

7.3.6 the specific duties of the Records Manager are contained in the Records Manager's job description which is on the case file.

7.3.7 the Records Manager is mandated to make such training and other interventions as are necessary to ensure that the Department record keeping and records management practices comply with the records management principles contained in the National Archives and Records Service Act.

7.3.8 the Records Manager may from time to time issue circulars and instructions regarding the record keeping and records management practices of the Department.

7.3.9 the Records Manager shall 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 National Archives and Records Service.

7.3.10 the Director, Information and Records Management is the Records Manager for the whole Department.

7.4 IT Manager

7.4.1 The IT Manager is responsible for the day-to-day maintenance of electronic systems that stores records.

7.4.2 The IT Manager should provide electronic facilities 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 shall 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 shall ensure that electronic systems capture appropriate systems generated metadata and audit trail data for electronic records to ensure that authentic and reliable records are created.

7.4.5 The IT Manager shall ensure that electronic records in 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 shall 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 shall ensure that back-ups are stored in a secure off-site environment.

7.4.8 The IT Manager shall ensure that systems that manage and store records are virus free.

7.4.9 Comprehensive details regarding specific responsibilities of the IT Manager are contained in:

7.4.10 the Electronic Records Management Policy

7.4.11 the E-mail policy

7.4.12 the Web content management policy

7.4.13 document imaging policy

7.4.14 Information security policy.

7.5 Security Manager

7.5.1 The Security Manager is responsible for the physical security of all records.

7.5.2 Details regarding the specific responsibilities of the security manager are contained in the information security policy.

7.6 Registry staff

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

7.6.2 Detailed responsibilities regarding the day-to-day management of the records in the registry are contained in the *Registry Procedure Manual.*

7.7 Staff

7.7.1 Every staff member shall create records of transactions while conducting official business.

7.7.2 Every staff member shall manage those records efficiently and effectively by:

7.7.3 Allocating reference numbers and subjects to paper-based and electronic records according to the file plan.

7.7.4 Sending paper-based records to the registry for filing.

7.7.5 Ensuring that records are destroyed/deleted only in accordance with the written disposal authority issued by the National Archivist.

8. IDENTIFICATION OF RECORDS

All records that are created or received by the Department in pursuance of its activities shall be managed in accordance with the provision of this policy.

9. CLASSIFICATION OF RECORDS

9.1 The Department shall use records classification systems approved by the National/Provincial Archives in line with legislation. This provision shall affect both electronic and paper based records. No employee shall make a revision or addition to an approved classification system without the prior approval by the Head of Department on the recommendation of Records Manager.

9.2 All official matters requiring the application of security measures (exempted from disclosure) must be classified "Confidential", "Secret" or "Top Secret". Security measures are not intended and should not be applied to cover up maladministration, corruption, criminal actions, etc., or to protect individuals/officials involved in such cases.

10. DISPOSAL OF RECORDS

10.1 No public records (including e-mail) shall be destroyed, erased or otherwise disposed of without prior written authorization from the National/Provincial Archivist.

10.2 The National/Provincial Archivist issues Disposal Authority Number for the disposal of records classified against the file plan. The Records Manager manages the disposal schedule.

10.3 The National/Provincial Archivist issues Disposal Authority Number on the schedule of records other than correspondence systems. The Records Manager manages the disposal schedule.

10.4 Retention periods indicated on the file plan and schedule were determined by taking Department 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.

10.5 Disposal in terms of these disposal authorities will be executed annually through shredding, recycling or burning.

10.6 All disposal actions should be authorized by the Records Manager prior to their execution to ensure that archival records are not destroyed inadvertently.

10.7 Non-archival records that are needed for litigation, Promotion of Access to Information requests or Promotion of Administrative Justice actions may not be destroyed until such time that the Deputy Information Officer has indicated that the destruction hold can be lifted.

10.8 Paper-based archival records shall be safely kept in [name of storage area] until they are due to transfer to the National/Provincial Archives Repository. Transfer procedures shall be as prescribed by the National/Provincial Archives in the Records Management Policy Manual.

10.9 Specific guidelines regarding the procedure to dispose of electronic records should be contained in the electronic records management policy.

11. CUSTODY AND STORAGE

11.1 The Records Manager of the Department shall ensure proper custody of all records including records with archival value prior to submission to archives.

11.2 The Records Manager must ensure the existence of Registry Office for keeping of records and that off-site storage must be approved by the National Archives.

11.3 The Records Manager must ensure that Registry Procedure Manual is in place as a guide on Registry Procedures.

11.4 The Records Manager must ensure that a reliable back up system for records is in place.

11.5 The Records Manager of the Department shall ensure proper custody of all records including records with archival value prior to submission to archives.

11.6 The Records Manager must ensure the existence of Registry Office for keeping of records and that off-site storage must be approved by the Provincial Archives.

11.7 The Records Manager must ensure that Registry Procedure Manual is in place as a guide on Registry Procedures.

11.8 The Records Manager must ensure that a reliable back up system for records is in place.

12. ACCESS AND SECURITY

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

12.2 Security classified records shall be managed in terms of the Minimum Information Security Standards.

12.3 No staff member shall remove records that are not available in the public domain from the premises of Department without the explicit permission of the Records Manager in consultation with the information security manager.

12.4 No staff member shall provide information and records that are not in the public domain to the public without consulting the Deputy Information Officer. Specific guidelines regarding requests for information are contained in the Promotion of Access to Information Policy which is maintained by the Deputy Information Officer.

12.5 Personal information shall be managed in terms of the Promotion of Access to Information Act until such time that specific protection of privacy legislation is enacted.

12.6 No staff member shall disclose personal information of any member of staff or client of the Department to any member of the public without consulting the Deputy Information Officer first.

12.7 An audit trail shall be logged of all attempts to alter/edit electronic records and their metadata.

12.8 Records storage areas shall at all times be protected against unauthorized access and shall be locked when not in use.

13. PAPER-BASED RECORDS

13.1 No records shall be removed from paper-based files without the explicit permission of the Records Manager.

13.2 Records that were placed on files shall not be altered in any way.

13.3 No alterations of any kind shall be made to records other than correspondence files without the explicit permission of the Records Manager.

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

14 TRAINING

14.1 The Records Manager shall successfully complete the National 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.

14.2 The Records Manager shall identify training courses that are relevant to the duties of the records management staff and shall ensure that the records management staff is trained appropriately.

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

15 INSPECTION OF RECORDS

15.1 In order for the Provincial/National Archives to conduct inspections as provided for by Section 13(2)c of the National Archives and Records Act, all Departmental units should, subsequent to consultations with the HoD, provide access for authorized NARS officials to records in their custody.

15.2 Records Management Unit shall conduct records inspection in institutions on a regular basis and advice the heads of institutions about the conditions under which records are managed.

15.3 Records Management Unit at the Provincial Office shall conduct

records inspections in all institutions (including the provincial Office) on a regular basis and advice the HoD through the office of the Director: Records Management about the conditions under which records are managed.

15.4 The Records Management Unit shall inspect and verify all records due for destruction.

15.5 Reports of all audits/inspections shall be managed in line with this policy.

16. REQUESITION OF INFORMATION

The Records Manager shall interact with the Deputy Information Officer designated by the Head of Department in terms of Section 17 of the Promotion of Access to Information Act in all matters related to requests, approval, providing, refusal and appeals in terms of the said Act.

17. REVIEW AND TERMINATION OF THE POLICY

The policy will be reviewed every 36 months based on the comments and inputs from the stakeholders and it will be terminated upon the inception of the new policy.

18. DEFAULT

Any person who contravenes the provision of the policy and the Registry Procedure Manual will be dealt with in terms of the penalty clause of the agreement entered into by and between him/her and the Department.

19. INCEPTION DATE

The inception date of this policy will be within 30 days after the approval by the Executive Authority.

20. ENQUIRIES

Enquiries regarding this policy should in the first instance be directed to the Records Management Directorate.

RECOMMENDED/~~NOT RECOMMENDED~~

For approval

____

____

____

ACCOUNTING OFFICER

18/8/17

DATE

APPROVED /~~NOT APPROVED~~

____

____

____

N. Ndalana

MEMBER OF EXECUTIVE COUNCIL

21/08/2017

DATE