RECORDS MANAGEMENT POLICY

DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

CONTENT

Definitions

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.

Classified information:

Classification given to information that may be used by hostile / opposing / malicious elements to disrupt the objectives and functions of an institution and / or state.

Confidential information:

Should be limited to information that may be used by hostile / opposing / malicious elements to harm the objectives and functions of an individual and / or institution

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 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.

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.r.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:

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.

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.

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.

Secret information:

Classification given to information that may be used by hostile / opposing / malicious elements to disrupt the objectives and functions of an institution and / or state.

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.

Top Secret information:

Classification given to information that can be used by enemies or hostile / opposing / malicious elements to neutralize the objectives and functions of institutions and / or state.

1. Purpose

1.1 Section 13 of the National Archives and Records Service of South Africa Act, 1996 requires the Department of Arts, Culture, Sports and Recreation to manage its records in a well-structured record keeping system, and to put the necessary policies and procedures in place to ensure that it's record keeping and records management practices comply with the requirements of the Act.

1.2 Information is a resource of the same importance to good management as other standard resources like people, money and facilities. The information resources of Department of Community Safety and Transport Management must therefore be managed as a valuable asset. Appropriate records management is a vital aspect of maintaining and enhancing the value of this asset. Department of Community Safety and Transport Management considers its records to be a valuable asset to:

- enable Department of Community Safety and Transport Management to find the right information easily and comprehensively;
- enable Department of Community Safety and Transport Management to perform its functions successfully and efficiently and in an accountable manner;
- support the business, legal and accountability requirements of Department;
- ensure the conduct of business in an orderly, efficient and accountable manner;
- ensure the consistent delivery of services;
- support and document policy formation and administrative decision-making;
- provide continuity in the event of a disaster;
- protect the interests of Department of Community Safety and Transport Management and the rights of employees, clients and present and future stakeholders;
- support and document the Department's activities, development and achievements;
- provide evidence of business in the context of cultural activity and contribute to the cultural identity and collective memory.

1.3 Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater co-ordination of information and storage systems.

2. Policy statement

2.1 All records created and received by Department shall be managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act, 43 of 1996.

2.2 The following broad principles apply to the record keeping and records management practices of the Department of Community Safety & Transport Management:

- The Department follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.
- The records management procedures of Department comply with legal requirements, including those for the provision of evidence.
- The Department follows sound procedures for the security, privacy and confidentiality of its records.
- Electronic records in the Department are managed according to the principles promoted by the National Archives and Records Service.
- The Department has performance measures for all records management functions and reviews compliance with these measures.

3. Relationship with other policies

3.1 The Department's Records Management Policy consist of this policy as well as additional parts that cover the unique nature of the broad spectrum of records generated by the Department. These policies are managed by the records manager. The following parts exist:

- Electronic records management policy
- E-mail policy;
- Document imaging; and

- Web content management policy

3.2 Other policies that are closely related to the Records Management Policy are
- the Information Security Policy which is managed by the Security Manager;
- the Internet Usage Policy which is managed by the IT Manager; and the
- Promotion of Access to Information Policy which is managed by the

4. Scope and intended audience

4.1 This policy impacts upon Department's work practices for all those who:
- create records including electronic records;
- have access to records;
- have any other responsibilities for records, for example storage and maintenance responsibilities;
- Have management responsibility for staff engaged in any these activities; or manage, or have design input into, information technology infrastructure.

4.2 The policy therefore applies to all staff members of Department and covers all records regardless of format, medium or age.

5. Regulatory framework

5.1 By managing its paper-based records effectively and efficiently Department strives to give effect to the accountability, transparency and service delivery values contained in the legal framework established by:
- **Schedule 5 Part A and section 195 of RSA Constitution Act , 1996 (Act 108 of 1996)**
- **National Archives and Records Service of South Africa Act (Act No 43 of 1996 as amended);**
  - **National Archives and Records Service of South Africa Regulations; R1458 of 2002**
- **Public Finance Management Act (Act No 1 of 1999);**
  The purpose of the act is to regulate financial management in the government and to prevent corruption.
  Efficient records management practices are imperative if a body want to give effect to the provisions of this act.
- **Promotion of Access to Information Act (Act No 2 of 2000);**
  The Act gives effect to the access to information right in the 1996 Constitution, section 32. The procedure to have Access to Information is contained in the Section 14 Manual of Department, promulgated in Government Gazette 37227, dated 16 January 2014. Section D of the promulgated Manual list the categories of Records Automatically available / Voluntary Disclosure. In terms of section 15 of PAIA the following archives and records are automatically open:
  Archives:
  - ✓ Public records in archival custody which are older than 20 years in age
  - ✓ Records of court proceedings and deceased estates
  - ✓ Non-public records acquired without stipulation of conditions of access

  Internal Records:
  - ✓ Registers of applications of disposal authority
  - ✓ Registers of disposal authorities issued
  - ✓ Registers of draft file plans submitted
  - ✓ Case files for disposal investigations, 1941-date
  - ✓ Indices of registrations of heraldic representations, names, uniforms and badges.
- **Promotion of Administrative Justice Act (Act No 3 of 2000);**
  To enable governmental bodies to comply with the provisions of this Act, they would keep proper records of administrative actions and decisions.
- **Electronic Communications and Transactions Act (Act No 25 of 2002)**
  To provide for the facilitation and regulation of electronic communications and transactions.

- **Public Finance Management Act, Act 1 of 19993**
  Sections 40 (1)(a) of the PFMA stipulates that the accounting officer is responsible for managing the financial administration of the department, and must take all reasonable steps to ensure that full and proper records of the financial affairs of the department are kept in accordance with any prescribed norms and standards.

- **Protection of Personal Information Act, Act 4 of 2013**
- **Minimum Information Security Standards (MISS)**
- **Minimum Physical Security Standards (MPSS)**
- **Electronic Communication and Transaction Act 25 of 2000**
- **Regulation of interception of communication and provision of communication-related information Act 70 of 2002**
- **Copyright Act 98 of 1978**
- **National Cyber Security Policy Framework 2012**

6. Statutory duties and responsibilities

6.1 Head of Department: Accounting Officer

6.1.1 In terms of section 10 (1 -3) of National Archives and Records Services Regulations R1458 of 2002 except where otherwise provided, the head of department shall comply with all directives and instructions issued by National Archivist and pertaining to the management and care of public records.

6.1.2 In terms of section 40 (1) (c) (i) of the PFMA the Accounting Officer is responsible for the management of financial records, reports and statements and makes them available for auditing by the Auditor General in terms of section 188 of the Constitution.

6.1.3 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.

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

6.1.5 In terms of section 13(5) of the National Archives Act, Act 43 of 1996 the Accounting Officer shall designate the Records Manager in accordance with section 12 of the National Archives Regulations R1458 of 2002.

6.1.6 In terms of Section 14 (1) (a) and (b) of PAIA the Accounting Officer is the Information Officer appointed in terms of section 1 (b)of the Promotion of Access to Information Act is obligated to submit:

- Section 32 reports to the SA Human Rights Commission
- Compile and submit Section 14, PAIA, Manuals
- Submit the list of Records automatically available in terms of section 15 of PAIA
  to the Minister of Justice.

6.1.7 In terms of the Minimum Information Security Standards, 1996 (MISS), the Accounting Officer or his delegate should ensure the overall security (i.e. physical and information security) of the Department and therefore should:

6.1.7.1 Develop and implement a Security Plan and Security Policy within the Department.

6.1.7.2 Ensure that employees have undergone security screening investigation and

Ensure that employees are re-vetted every 5 years in cases of Secret and Top Secret clearances and 10 years in the case of confidential clearances.

6.2 Statutory duties of National or Provincial Archivist

6.2.1 In terms of Section 13(2)(b) of the National Archives Act, Act 43 0f 1996, the Provincial Archivist shall valuate, approve and monitor the implementation of the approved record classification system.

6.2.2 The Provincial Archivist must issue and approve disposal authorities and approve destruction and transfer of records

6.2.3 The Provincial Archivist must conduct Records Management inspection at the Department and for such inspection the Accounting Officer must grant access to the Provincial Archivist to Records to be inspected to ensure compliance and proper Records Management.

6.2.4 The Provincial Archivist must appraise Records and issue disposal authorities thereof.

6.2.5 The Provincial Archivist must provide training in Archival techniques and Management of Records in terms of section 5(2)(a) of the National Archives Act, Act 43 of 1996.

6.2.6 The Provincial Archivist should determine the conditions subject to which electronic records systems should be managed.

6.2.7 The Provincial Archivist must collect, arrange, describe and preserve A20 or records that have endure value or A20 in the archives repository in terms of section 11 of the National Archives Act, Act 43 of 1996.

6.2.8 The Provincial Archivist must make the Records accessible for consultation by the researchers or users in terms of section 12 of the National Archives Act, Act 43 of 1996.

6.2.9 The Provincial Archivist must conduct Public outreach or awareness programmes in terms of section 5(1) (c) of the National Archives Act, Act 43 of 1996

6.2.10 In terms of section 14(1) of the National Archives Act, Act 43 of 1996 the Provincial Archivist may acquire by purchase or donation or on loan for a temporary period or in perpetuity, either unconditionally of subject to such conditions as may be agreed upon, non-public records which, in his or her opinion, have enduring value of national significance and which cannot be more appropriately preserved by another institution.

6.3 Roles and Responsibilities of the Records manager:

6.3.1 **File Plans:**

The records manager is responsible for the overall control over the compilation, implementation, maintenance and utilization of approved file plans and the records file according to these systems. During the compilation of a new file plan the records manager should liaise with the Provincial Archives and Records Service for assistance and advice during the process. Once the file plan has been compiled, the records manager should submit it to the Provincial and National Archivist for approval. The records manager should keep a master copy of the file plan updated to always reflect the functions of the body. The records manager must ensure that the approved file plan is maintained and that all additions and amendments are reported to the Provincial Archivist. As the functions and activities of a body develop, a similar development should occur in the file plan. The records manager should ensure that changes in the file plan are reflected in the physical files and in the electronic system if the body is using an electronic system.

The records manager should ensure that the registry staff is trained in the allocation of reference numbers and in file plan maintenance procedures. The records manager should also ensure that all the users of the system are trained to allocate reference numbers to correspondence, to ensure that records are not misplaced. Supervisions over the implementation and maintenance of the filing system (the storage system for records) must be ensured. The correct placement of documentation should be monitored and particular attention should be paid to policy, archival, routine enquiry and parent files in both the paper-based and the electronic system to ensure that they are used correctly.

6.3.2 **Schedule of records other than correspondence systems**:

The records manager is responsible for the overall control over the compilation, maintenance and utilization of the approved schedules for records other than correspondence systems as well as the records themselves.

The records manager must ensure that the schedule for other records systems is compiled and submitted in duplicate to the Provincial Archivist for the issuing of a disposal authority. The records manager should ensure that the master copy of the schedule is maintained and updated and must ensure that all revisions and additions are reported to the Provincial Archivist, to facilitate the issuing of a disposal authority for the records.

The records manager should ensure that the disposal authority is applied at least once a year to ensure that archival records are transferred into archival custody and that non-archival records no longer needed are destroyed. The records manager should also ensure that all staff is aware of the penalty for the unauthorized destruction or mismanagement of records.

6.3.3 **Destruction of records**:

The destruction of non-archival records must occur in the presence of the records manager. He/she must before destroying non-archival records ensure that:

- ✓ No work is outstanding
- ✓ No litigation or investigation is being conducted which concerns the records in question
- ✓ The records have not been requested in terms of the Promotion of Access to Information Act or the Promotion of Administrative Justice Act.

The records manager must also ensure that destruction of archival records does not occur.

Records managers must ensure that all destruction actions are properly documented. They must submit destruction certificates to the Provincial Archivist once records have been destroyed and ensure that the body keeps a record of all destruction actions taken regarding records.

6.3.4 **Transfer of records:**

The records manager should supervise the transfer of the archival records to an appropriate archives repository when the time is right.

The records manager must inform the Provincial Archivist in writing when records are permanently transferred to another governmental body. A complete list of the records should also be submitted to the Provincial Archivist.

The records manager must ensure that no public records are transferred to off-site storage facilities without the permission of the Provincial Archives and Records Service. The records manager, in conjunction with Provincial Archives and Records Service's Records Management Division, should inspect the off-site

storage facility before any records are transferred into its custody. The records manager should inspect the facility regularly after transfers have taken place. The records manager should notify the Provincial Archivist when such inspections are planned and should submit copies of the inspection reports to the Provincial Archivist. The records manager should ensure that the off-site storage facility is familiar with the requirements of the Provincial Archives and Records Service Act before records are transferred into its custody.

The records manager should ensure that no records are transferred, whether permanently or temporarily, to any person or institution outside of government unless the national Archivist has been informed at least sixty days beforehand and written authorization has been granted.

6.3.5 **Records in all formats:**

The records manager is responsible for ensuring the safe custody and storage of all records in all formats.

The records manager should conduct regular inspections in the individual components to ensure that their records management practices conform to the standards promulgated in the Act. Copies of these reports should be submitted to the Provincial Archivist. The records manager should liaise with the IT manager to share information regarding the proper storage of electronic records and should be involved in the regular maintenance of records stored on electronic storage media. He/she should ensure that regular inspections are done and that the results of these inspections are also reported to the Provincial Archives and Records Service.

Buildings and storage areas should be regularly monitored in order to maintain a stable, protective environment for records. The records manager should develop a programme whereby the building, temperature, humidity, air quality, and light in storage areas are monitored, pests are controlled, fire protection and safety equipment are checked and the presence of magnetic fields is monitored. The records manager should also inspect the records themselves to monitor for signs of deterioration.

The records manager should ensure that a proper disaster management programme is in place and communicated throughout the organization.

The records manager should ensure that all staff are aware of the importance of security in the building and records storage areas.

6.3.6 **Training:**

The records manager is responsible to implement and manage a suitable training programme for managers, employees, contractors and records management staff. He/she should supervise the training of staff regarding records management matters and regularly evaluate the success of the training programme against the effectiveness of the records management programme.

The records manager should ensure that records management consultants and suppliers of electronic records management and related products employed by the governmental body are familiar with the requirements of the national Archives and Records Service Act.

Every registry in a governmental body should have a registry procedure manual to facilitate the training of registry staff.

The records manager is responsible for ensuring that the registry head is trained and has attended the Provincial Archives and Records Service's Records Management Course. He/she should ensure that the registry head and registry

staff are aware of and adhere to the standards, procedures and methods of records management promulgated in the National Archives and Records Service of South Africa Act.

The records manager is responsible to ensure that all staff members are made aware of their joint responsibility in maintaining sound records management practices. He/she should conduct awareness campaigns in this regard.

The records manager should arrange with the Provincial Archives and Records Service's Records management Division to conduct implementation workshops whenever new file plans are implemented to ensure that all members of staff know how to read and use the file plan.

6.3.7 **Qualifications of the Records Manager**

In Terms of section 13(5) of the National Archives and Record Service of SA Act, Act 43 of 1996, and section 12 of the National Archives and Record Service of SA Regulations, the Records Manager of a governmental body, shall have the following qualification:

- Be in possession of an appropriate university or University of Technology qualifications and/or have appropriate professional experience;
- Have successfully completed the National Archives Records Management course;
- Possess a thorough knowledge of the body's organizational structure, functions and records system, and
- Be responsible for promoting the effective and accountable management of the body's records and ensuring, by inspection and other means, the body's compliance with the Act and all other relevant legislation.

6.3.8 **Status of the Records Manager in the organization:**

The following criteria should be applied regarding the positioning of the Records Manager in the organization:

- The official should occupy a relatively central position in the organization
- The official should occupy a senior enough position to ensure ready liaison with division heads and senior management
- The official should be able to make responsible decisions concerning all aspects of records management practices and implement them to the highest level in the office.
- It is therefore undesirable for the Registry Head and the Records manager to be one and the same person.
- Where an office has sub-offices or comprises several departments or divisions, a Records Manager should be appointed for each component. These officials should be answerable to a Records Manager for the body, i.e. an overall Records manager for the body as a whole.

6.3.9. **Non-delegatable duties of the Records Manager:**

To prevent the delegation of authority the following non-delegatable duties should be assigned to the Records Manager and the following duties should be reflected on the official's duty sheet:

- Control over the maintenance and application of the filing system and Records Control Schedule
- Disposal of all records
- Safe custody of all records
- Control over staff in the registry, and
- Application of policy of document economy.

The specific duties assigned to the Records manager flow from the foregoing.

6.3.10 **Records Classification Systems**:

i) Ensure that the filing systems, Records Control Schedules and classification systems for electronic systems of all components the body is submitted to the Provincial Archivist for approval.
   - ✓ Compilation of new Records Classification Systems
   - ✓ Keeping Master Copies
   - ✓ Maintenance of filing system

i) Disposal Authority
ii) Transfer of records to appropriate archives repository or records centre's
iii) Destruction Certificates
iv) Inspection by Officials of the Provincial Archives
v) Surveys by Officials of the Provincial Archives
vi) Inspections by the Records manager
vii) Physical Care
viii) Registry Procedure Manuals
ix) Training and Selection of Staff

6.4 Chief Information Officer

6.4.1 The Chief Information Officer is responsible for approval of requests for information in terms of the Promotion of Access to Information Act.

6.4.2 The Chief Information Officer shall inform the records manager if a request for information necessitates a disposal hold to be placed on records that are due for disposal.

6.5 IT manager

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

6.5.2 The IT manager shall 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.

6.5.3 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.

6.5.4 The IT manager shall 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.

6.5.5 The IT manager shall 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.

6.5.6 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.

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

6.5.8 The IT manager shall ensure that systems that manage and store records are virus free.

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

- the E-mail policy;
- the Web content management policy;
- document imaging policy; and the
- Information security policy.

6.6 Security manager

6.6.1 The security manager is responsible for the physical security of all records.

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

6.6.3 Minimum Information Security Standards, 1996 requires that Employees or applicants and Service Providers who/that will have access to classified information intelligence in the possessions of the Department should undergo security screening investigations or security screening to determine the security competence of the employee.

6.7 Legal services manager

The legal services manager is responsible for keeping the Records Manager updated about developments in the legal and statutory environment that may impact on the record keeping and records management practices of Department.

6.8 Registry Head

The following tasks are entrusted to the Registry Head and should be recorded in the duty sheet:

- Opening of files and replacement of worn covers
- Responsible for noting the correct reference number on all incoming correspondence and other material
- Responsible for the correct and neat filing of all material
- Keeps control over the filing to prevent unnecessary duplicates of bulky items being placed on the files
- Responsible for the custody of keeping of:
  - ✓ A register of files opened
  - ✓ A destruction register and
  - ✓ A register of authorities
- Responsible for all amendments/additions being brought to the notice of interested parties
- Responsible for the closure of records
- Controls the receipt and opening of post
- The recording of moneys and valuable documents that are received
- The tracing of files
- The despatch of outgoing items
- The pending of correspondence
- The training of registry personnel.

6.9 Staff

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

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

- allocating reference numbers and subjects to paper-based and electronic records according to the file plan;
- sending paper-based records to the registry for filing;
- Ensuring that records are destroyed/deleted only in accordance with the written disposal authority issued by the Provincial Archivist.

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

7. Records classification systems and related storage areas

The Department of Community Safety & Transport Management has the following systems that organize and store records:

7.1 Correspondence systems

7.1.1 File plan

7.1.1.1 Only the file plan approved on [date] and implemented on [date] shall be used for the classification of correspondence records. The file plan shall be used for the classification of paper-based and electronic (including e-mail) records.

7.1.1.2 Specific procedures for the allocation of file subjects and reference numbers to electronic records are contained in the [name of system] procedures manual that is published on the Intranet, filed on file. More specific guidance regarding the classification of e-mail is contained in the E-mail management policy that is published on the Intranet, filed on file from the Department file plan.

7.1.1.3 Each staff member shall allocate file reference numbers to all correspondence (paper, electronic, e-mail) according to the approved subjects in the file plan.

7.1.1.4 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. Specific procedures regarding the addition and approval of a subject in the electronic system are contained in the procedures manual that is published on the Intranet and filed.

7.1.2 Storage areas

7.1.2.1 Paper-based correspondence files are kept in the custody of-

7.1.2.1.1 The central registry

7.1.2.1.1.1 All paper-based correspondence system records that are not HR related are housed in the central registry.

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

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

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

7.1.2.1.1.5 The registry shall be locked when registry is not in operation.

7.1.2.1.2 The Human Resources registry

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

7.1.2.1.2.2 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.

7.1.2.1.2.3 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.

7.1.2.1.2.4 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.

7.1.2.1.2.5 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

7.1.2.2 Electronic correspondence records are stored in an electronic repository that is maintained by the IT section.

7.1.2.2.1 Access to storage areas where electronic records are stored is limited to the Information Technology staff that has specific duties regarding the Maintenance of the hardware, software and media.

7.2 Records other than correspondence systems

7.2.1 Schedule for records other than correspondence systems

7.2.1.1 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. The schedule is available on the Intranet and filed.

7.2.1.2 Should records be created/received that are not listed in the schedule, the records manager should be contacted to add the records to the schedule.

7.2.2 Storage areas

7.2.2.1 Paper-based

7.2.2.1.1 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.

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

7.2.2.2 Micrographic records

7.2.2.2.1 The Department has sets of microfilmed records that are stored in the IT section.

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

7.2.2.3 Audio-visual records

7.2.2.3.1 The Department has sets of audio-visual records that are stored in the IT section, archives repository, communication sections

7.2.2.4 Electronic systems other than the correspondence systems

7.2.2.4.1 The Department has a number of electronic records systems in operation which is not part of the correspondence system and that generate and store public records.

7.2.2.4.2 The IT manager is responsible for the day-to-day maintenance of these systems.

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

7.2.2.4.4 Detailed guidance regarding the management of these systems is contained in the electronic records management policy.

7.2.3 Management of Classified information in terms of MISS

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

- State Secret
- Trade Secret
- Personal Information

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

- Confidential
- Secret
- Top Secret

7.2.3.2 Employees of the Municipality who generates sensitive information are responsible for determining information classification levels and the classification thereof, subject to management review. This responsibility includes the labeling of classified documents.

7.2.3.3 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. Classification levels assigned to information should strictly be observed and may not be changed without the consent of the Accounting Officer or his delegate.

7.2.3.4 Access to classified information will be determined by the following principles:
Intrinsic secrecy approach
Need-to-know principle

- Level of security clearance

7.2.3.5 Classified Information should be stored in following manner:
Confidential Documents should be store in a reinforced filing cabinet;
Secret Documents should be stored in a safe of strong room (walk-in-Safe), and
Top Secret Documents should be stored in a safe or strong room (walk-In-safe)

8. Disposal of records

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

8.2 The Provincial Archivist shall issue Standing Disposal Authority Number for the disposal of records classified against the file plan. The records manager manages the disposal schedule. (To be obtained, after approval)

8.3 The Provincial Archivist issue Standing Disposal Authority Number on the schedule of records other than correspondence systems. The records manager manages the disposal schedule.

8.4 Retention periods indicated on the file plan and schedule will be determined by taking 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.

8.5 Disposal in terms of these disposal authorities will be executed annually in December.

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

8.7 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 Manager: Legal Services has indicated that the destruction hold can be lifted.

8.8 Paper-based archival records shall be safely kept until they are due to transfer to the Provincial Archives Repository. Transfer procedures shall be as prescribed by the National Archives in the *Records Management Policy Manual.*

8.8 Specific guidelines regarding the procedure to dispose of electronic records are contained in the electronic records management policy.

9. Storage and custody

9.1 See par. 7 for an identification of all record keeping systems and their storage locations.

9.2 All records shall be kept in storage areas that are appropriate for the type of medium. The National Archives and Records Services' guidelines contained in the *Records Management Policy Manual* shall be applied.

9.3 Specific policies for the management of electronic storage media are contained in the electronic records management policy.

9.4 PHYSICAL SECURITY

9.4.1 Physical security involves the proper layout and design of Community Safety and Transport Management and the use of physical security measures to delay and prevent unauthorized access to confidentiality of assets of the department. It includes measures to detect attempted or actual unauthorized access and activation of an appropriate response. Physical security also includes the provision of measures to protect employees from bodily harm.

9.4.2 Physical security measures must be developed, implemented and maintained in order to ensure that the entire department, its personnel, property and information are secured. These security measures shall be

based on the findings of the Thread and Risk Assessment (TRA) to be conducted by the SM.

9.4.3 The SM shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities.
The Department of Local Government and Traditional Affairs shall:

- Select, design and modify facilities in order to facilitate the effective access control thereof.
- Demarcate restricted access areas and have the necessary entry barriers, security and equipments to effectively control access thereto;
- Include the necessary security specifications in planning, request for proposals and tender documentation
- Incorporate related costs in funding requirements for the implementation of the above.

9.4.4 The Municipality will also ensure the implementation of appropriate physical security measures for the source storage, transmittal and disposal of classified and protected information in all forms

9.4.5 All employees are required to comply with access control procedures of the department at all times.

10. Access and security

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

10.2 Security classified records shall be managed in terms of the Information Security Policy which is available from the security manager.

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

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

10.5 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.

10.6 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 Chief Information Officer first.

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

10.8 Records storage areas shall at all times be protected against unauthorized access. The following shall apply:

10.8.1 Registry and other records storage areas shall be locked when not in use.

10.8.2 Access to server rooms and storage areas for electronic records media shall be managed with access control.

11. Legal admissibility and evidential weight

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

11.1.1 Paper-based records

11.1.1.1 No records shall be removed from paper-based files without the explicit permission of the records manager.

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

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

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

11.1.2 Electronic records

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

- authentic;
- not altered or tampered with;
- auditable; and
- produced in systems which utilize security measures to ensure their integrity.

11.1.2.3 The Electronic Records Management Policy contains specific information regarding the metadata and audit trail information that should be captured to ensure that records are authentic.

12. Training

12.1 The records manager shall successfully complete the Provincial 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.

12.2 The records manager shall identify such training courses that are relevant to the duties of the registry staff and shall ensure that the registry staff is trained appropriately.

12.3 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.

13. Monitor and review

13.1 The records manager shall review the record keeping and records management practices of the Department on a regular basis and shall adapt

them appropriately to ensure that they meet the business and service delivery requirements of the Department.

13.2 This policy shall be reviewed on a regular basis and shall be adapted appropriately to ensure that it meets the business and service delivery requirements of Department.

14. References

Department of Public Service and Administration: *Draft Information Security Policies. Securing Information in the Digital Age.*

National Archives and Records Service: *Records Management Policy Manual*, April 2006.

National Archives and Records Service: *Managing electronic records in governmental bodies: Policy, principles and requirements,* April 2006.

National Archives and Records Service: *Performance criteria for records managers in governmental bodies*, April 2006.

National Intelligence Agency: *Minimum Information Security Standards.*
South African Police Services: Minimum Physical Security Standards

South African Bureau for Standards: SANS 15489: *Information and documentation – Records management – Part 1: General.*

South African Bureau for Standards: SANS 15489 *Information and documentation – Records management – Part 2: Guidelines.*

South African Bureau for Standards: SANS 15801: *Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability.*

South African Bureau for Standards: SANS 23081: *Information and documentation – Records Management processes – Metadata for records – Part 1: Principles.*

South African Bureau for Standards: SANS 17799: *Information Technology – Security techniques - Code of Practice for Information Security Management.*

15. Endorsement and approval

The evaluation and endorsement of this policy will be done by North West Provincial Archives and Records Services. The approval will be done by Head of Department of Arts, Culture, Sports and Recreation.

Policy endorsed by

.....

Mr S.I Mogorosi
HEAD OF DEPARTMENT: ACSR

16/10/2023
.....
Date

This policy was approved by

.....

Dr H Kekana
HEAD OF DEPARTMENT: COSATMA

14/11/2023
.....
Date