KWAZULU-NATAL PROVINCE

HUMAN SETTLEMENTS
REPUBLIC OF SOUTH AFRICA

RECORDS MANAGEMENT POLICY

Version	**5**
Applicability	**All departmental employees**
Approval history	**08th April 2014,16 January 2017 & 17th February 2020**
Last date of approval	**23rd June 2022**
Period of review	**As and when required**
Owner Business Unit	**General Administration & Auxiliary Services (GAAS)**

Table of Content

1. DEFINITIONS 3-5
2. PURPOSE 5
3. POLICY STATEMENT 6
4. POLICY IDENTIFICATION 6
5. SCOPE AND INTENDED AUDIENCE 6
6. REGULATORY FRAMEWORK.....7
7. ROLES AND RESPONSIBILITIES 7

    7.1 HEAD OF DEPARTMENT 7
    7.2 SENIOR MANAGEMENT.....7
    7.3 RECORDS MANAGER 7-8
    7.4.DEPUTY INFORMATION OFFICER.....8
    7.5. LEGAL SERVICES DIRECTOR.....8
    7.6. IMST DIRECTOR.....8-9
    7.7. REGISTRY STAFF 9
    7.8. STAFF IN GENERAL 9-10
    7.8 REGIONAL AND DISTRICT OFFICES.....10

8. RECORDS CLASSIFICATION SYSTEM AND RELATED AREAS...10

    8.1 FILE PLAN 10
    8.2 STORAGE AREAS 10-11
    8.3 RECORDS OTHER THAN CORRESPONDENCE FILES..... 11

9. DISPOSAL OF RECORDS 11-12
10. CUSTODY..... 12
11. ACCESS AND SECURITY 12
12. TRANSFER OF RECORDS..... 12
13. LEGAL ADMISSIBILITY AND EVIDENTIAL WEIGHT..... 13

    13.1 PAPER-BASED RECORDS 13
    13.2 ELECTRONIC RECORDS 13

14. CLASSIFICATION OF FILES.....13-15
15. TRAINING 15
16. INSPECTION BY THE KZN ARCHIVES.....16
17. PROCESSING OF PERSONAL INFORMATION.....16-20
18. MANNER OF ACCESS.....20
19. PROCESSING OF SPECIAL PERSONAL INFORMATION.....20-22
20. PROCESSING OF PERSONAL INFORMATION OF CHILDREN.....22
21. MONITOR AND REVIEW 22
22. REFFERENCES.....22
23. APPROVAL 23

1.Definitions of terms

Archives repository:
A 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.

Biometrics:
A technique of personal identification that is based on physical, physiological or behavioural charecterisation including blood typing fingerprinting, DNA analysis, retinal scanning and voice recognition.

Child:
A natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or her.

Competent person:
Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

Consent:
Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

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 on physical possession of a person/official/employee.

Data Subject:
Individual employees, service providers, community members, external members of governance structures and other stakeholders of whom the Department collects and processes their personal information.

Disposal:
The action of destroying, deleting or transferring records to archives 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 metadata (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.

Electronic communication:
Any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Person:
A natural person or a juristic person.

File plan:
A pre-determined classification plan in which records are filed and/or electronically indexed to facilitate efficient retrieval and disposal.

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.

Information owner / data subject:
The person to who personal information relates.

Non-archival records:
Records with a short lived interest or usefulness. These records have administrative value.

Personal information
Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) Information relating to the education or the medical, financial, criminal or employment history of the person;

(c) Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) The biometric information of the person;
(e) The personal opinions, views or preferences of the person;
(f) Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) The views or opinions of another individual about the person; and
(h) The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Processing:
Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteraction, consultation or use, dissemination by means of transmission, distribution or making available in any other form or merging, linking as well as restriction, degradation, erasure or destruction of information.

Public body:
Any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government of any other functionary or institution when exercising a power or performing a duty in terms of the Constitution or provincial constitution or exercising a public power or performing a public function in terms of any legislation.

Record:
1) Recorded information regardless of form or medium.
2) Evidence of a transaction, preserved for the evidential information it contains.

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.

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.

Special Personal Information:
The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information or the criminal behaviour of a Data Subject.

2. Purpose

2.1 Section 13 of the National Archives and Records Service of South Africa Act 43 of 1996 and KZN Archives and Records Service Act, 8 of 2011 requires the KZN Department of Human Settlements to manage its records in a well-structured record keeping system, and to put the necessary policies and procedures in place to ensure that its record keeping and records management practices comply with the requirements of the Acts.

2.2 To serve as a source of guidance for the management and usage of classified public records of the KZN Department of Human Settlements

2.3 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.

2.4 To ensure that the KZN Department of Human Settlements identifies, documents and manages records containing personally identifiable information in accordance with applicable privacy laws.

2.5 All departmental officials must comply with the provisions of this policy. Failure to comply with this policy shall lead to disciplinary action taken against the official/s.

3. Policy statement

3.1 All records created and received by the KZN Department of Human Settlements 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 as amended and section 18 of the KZN Archives and Records Services Act 8 of 2011 as well as the Protection of Personal Information Act (POPIA), 04 of 2013.

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

3.2.1. The KZN Department of Human Settlements follows sound procedures for the creation, maintenance, retention and disposal of all records, including electronic records.

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

3.2.3. The KZN Department of Human Settlements follows sound procedures for the integrity, security, privacy and confidentiality of its records.

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

3.2.5. The Department seeks to constantly improve records management practices in line with changing business and regulatory requirements.

3.2.6. Records which contain personal information in terms of POPIA will only be retained for the period for which they are required to fulfil the purpose for which they were gathered.

3.2.7. The KZN Department of Human Settlements has performance measures for all records management functions and reviews compliance with these measures.

3.3 The KZN Department of Human Settlement's Records Management Policy consists of this policy as well as other policies 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 policies should exist:

3.3.1. E-mail policy
The policy emphasizes staff awareness of the importance of e-mail correspondence as is regarded as public records. Printout of all communications should be filed to their respective reference numbers.

(exists with IMST)

3.3.2. Web Content Management Policy;- the update of the departmental web content in every change that takes place. (exists with IMST)

3.3.3. Information Security Policy. (exists with IMST)

3.3.4. Registry Procedure Manual. (exists with General Administration and Auxiliary Services)

4. Policy identification

4.1. The Records Management Policy for the KZN Department of Human Settlements emphasizes that all records created or received during the execution of department's functions are public records and must be managed in accordance with the determined policy guidelines.

4.2. It stipulates that public records must be effectively classified and stored so that they are easily accessible, thereby facilitating transparency, accountability and democracy.

5. Scope and intended audience

5.1 This policy impacts upon Departmental 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.

5.2 The policy therefore applies to all staff members of the KZN Department of Human Settlements and covers all records regardless of format, medium or age, all third parties who manage the Department's information in any manner and records at all stages of their life cycle, whether at rest, in transit, or in use.

5.3 Records covered by this policy relate to all recorded information in all formats used in relation to all aspects of the business of the KZN Department of Human Settlements. Electronic records have the same status as paper records. Both electronic and paper records are bound by the same legislative requirements and are subject to the same degree of confidentiality and care.

6. Regulatory framework

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

6.1.1. The Constitution of the Republic of South Africa, Act 108 of 1996;
6.1.2. National Archives and Records Service of South Africa Act (Act No 43 of 1996 as amended);
6.1.3. KZN Archives and Records Service Act, (Act 8 of 2011)
6.1.4. Public Finance Management Act (Act No 1 of 1999);
6.1.5. Promotion of Access to Information Act (Act No 2 of 2000);
6.1.6. Promotion of Administrative Justice Act (Act No 3 of 2000);
6.1.7. Electronic Communications and Transactions Act (Act No 25 of 2002)
6.1.8. Protection of Personal Information Act (Act 4 of 2013)
6.1.9. Minimum Information Security Standards (MISS)
6.1.10. The Treasury Regulations, section 17.

7. Roles and responsibilities

7.1 Head of Department (Information Officer)

7.1.1. The Head of Department is the ultimate accounting officer for the record keeping and records management practices of this Department as the Information Officer.

7.1.2. 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.

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

7.1.4. 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 Senior management

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

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

7.2.3. Senior management shall ensure that all staff in their units is aware of their record keeping and records management responsibilities and obligations.

7.2.4. Senior management shall ensure that the management of records including e-mail is a key responsibility in the performance agreements of all the staff in their units.

7.2.5. All correspondence shall reflect relevant file numbers from the approved records classification systems.

7.3 Records Manager

7.3.1. The Records Manager is responsible for:

7.3.1.1. Staff awareness regarding this policy;

7.3.1.2. The implementation of this policy;

7.3.1.3. The management of all records according to the records management principles contained in the National Archives and Records Service Act 43 of 1996 and the KZN Archives and Records Services Act 8 of 2011.

7.3.1.4. 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.

7.3.1.5. Records are effectively and correctly backed-up using the electronic system procured by the Department.

7.3.1.6. Sourcing off-site storage for records created by the department when the available space is not enough.

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

7.3.3 The Records Manager shall ensure that all records created and received by the KZN Department of Human Settlements are classified according to the approved file plan and that a written disposal authority is obtained from the KZN Archives and Records Service.

7.3.4 The Records Manager is the records manager for the whole Department of Human Settlements not unless there is a sub-records manager with defined areas of responsibility.

7.4 Deputy Chief Information Officer

7.4.1 The Deputy Chief Information Officer is responsible for approval of requests for information in terms of the Promotion of Access to Information Act 2 of 2000.

7.4.2 The Deputy 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.

7.5 Legal Services Director

7.5.1 The Legal Services Director 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 the KZN Department of Human Settlements.

7.6 IMST Director

7.6.1. The IMST Director is responsible for the day-to-day maintenance of electronic systems that store records.

7.6.2. The IMST Director shall work inconjuction with the Records Manager to ensure that electronic records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long term preservation purposes.

7.6.3. The IMST Director shall ensure that electronic records in all systems remain accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence.

7.6.4. The IMST Director 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.

7.6.5. The IMST Director shall ensure that electronic systems that manage and store records are virus free.

7.7 Registry staff

7.7.1 The registry staff is responsible for the physical management of all 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 Procedure Manual.*

7.7.3. Ensures compliance with this policy (*Records Management Policy).*

7.8 Staff in general

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

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

7.8.3. Allocating relevant reference numbers to paper-based and electronic records according to the file plan.

7.8.3.1 Sending paper-based records to registry for filing.

7.8.3.2. Ensuring that business units promote proper management of records and archives by adhering to relevant legislation and the provisions of this policy.

7.8.3.3. The Records Manager in consultation with other records designated employees will co-ordinate the implementation of the General File Plan and Human Resources File Plan as provided for in this policy.

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

7.8.4. **No official is allowed to release personal information of any departmental official or third party without express permission of such employee or third party.**

7.9 Regional and District Offices

7.9.1. The regional and district offices must have an appointed Records official who will report directly to the appointed Records Manager with the functions as stipulated in 7.3.

7.9.2. Each regional/district office must have a proper registry with all the required facilities (as stipulated in 8.2 below).

7.9.3. All registry functions will be entrusted to this official within the regional and district office.

7.9.4. All messenger services will be reported to Registry official within this office.

7.9.5. The regional and district offices use the approved records classification systems as used by the Head Office.

8. Records classification systems and related storage areas

8.1 File plans

8.1.1. Only the General and Human Resource File Plans as approved by the Head of Department shall be used for the classification of correspondence records in the Head Office and all other departmental offices. The file plan shall be used for the classification of paper-based and electronic (including e-mail) records.

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

8.1.3 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 general system are contained in the Registry Procedure Manual.

8.2 Storage areas

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

8.2.1.1. <u>The general registry</u>

8.2.1.1.1. All paper-based correspondence system records that are not HR related are housed at general registry.

8.2.1.1.2. All these records are under the management of the Records Manager who is mandated to ensure that they are managed properly.

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

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

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

8.2.1.1.6. The registry shall be centrally located for ease of access.

8.2.1.1.7. The registry shall be equipped with all the necessary equipment in effectively protecting the authenticity and confidentiality of records it housed.

8.2.1.1.8. The registry should be fire-proof to protect records against fire.

8.2.1.1.9. Shelving must 150 mm elevated from the floor and 300 mm away from the ceiling to allow for air flow.

8.2.1.1.10. Access to registry must be controlled by a security system allowing only registry staff to access registry.

8.2.1.1.11. Registry must have regularly serviced Carbon Dioxide (CO_2) fire extinguishers, which registry staff must be trained on how to use it.

8.2.1.2. The Human Resources registry

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

8.2.1.2.2. 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.

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

8.2.1.2.4. 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.

8.2.1.2.5. The files exist on paper-based and electronic format and the physical tracking of the case files are managed accordingly, using Metrofiler Business Entreprise a scanning system/ electronic back-up filing system.

8.2.1.2.6. Access to registry must be controlled by a lockable door and a service counter allowing only registry staff access.

8.3. Electronic correspondence records are stored in an electronic repository maintained by IMST.

8.3.1. Access to storage areas where electronic records are stored is limited to the IMST staff that have specific duties regarding the maintenance of hardware and media.

9.Disposal of records

9.1. Section 13 (2) (a) of the National Archives and Records Services Act 43 of 1996, as amended and section 18 (2) of the KZN Archives and Records Services Act 8 of 2011, stipulate that no public records (including e-mail) shall be destroyed, erased or otherwise disposed of without prior written authorization from the Provincial Archivist.

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

9.3. The Provincial Archivist also, issues Disposal Authority on the Records Control Schedule for records other than correspondence files (other records). The Records Manager manages the disposal schedule.

9.4. Retention periods to be indicated will be determined by taking the KZN Department of Human Settlements' 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.

9.5. Disposal in terms of these disposal authorities will be executed annually. The emphasis is on the fact that archival paper-based records must be kept for a period of 20 years before they are transferred to an archives repository, unless agreement on a shorter retention period has been reached with the Provincial Archivist

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

9.10. All original records covered by this policy should be disposed in a manner that they cannot be reconstructed into their intelligible form as prescribed by section 14(5) of POPIA.

9.11. A Certificate of Destruction must be produced by the Records Manager to record the reason for the destruction of the original file, to meet statutory and regulatory requirements. The Certificate of Destruction must contain the signatures of the office of origin, the relevant Deputy Information Officer and the Records Manager authorizing the physical destruction of the records. Certificates of Destruction must be retained indefinitely.

9.12. Unauthorized destruction or disposal of records or information may result in criminal prosecution and/or disciplinary action and where applicable, liability for damages and losses incurred by the KZN Department of Human Settlements.

9.13. Non-archival records that are needed for litigation, audit, pending investigations, or Promotion of Administrative Justice actions may not be destroyed until such time that the Director: Legal Services has indicated that the destruction hold can be lifted. These records will fall under the destruction moratorium which constitutes a "records hold". The destruction of these records should remain on hold until the legal proceedings have ceased and the time period for an appeal or review in terms of the legal proceedings has elapsed.

9.14. When a PAIA request for access to a record is received by the KZN Department of Human Settlements, all necessary steps must be taken to ensure that the relevant record is preserved in accordance with section 21 of PAIA, without deleting any information contained in it, until the Information Officer or Deputy Information Officer has notified the requester concerned of the decision on the request made.

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

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

10.Custody

10.1. See par 8 for an identification of all record keeping systems and their storage locations.

10.2. All records shall be kept in storage areas that are appropriate for the type of medium. The Provincial Archives and Records Services' guidelines in the *Records Management Policy* shall be kept.

11.Access and security

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

11.2. Security classified records shall be managed in terms of the Security Policy, which is available from the Security Manager.

11.3. No staff member shall remove records that are not available in the public domain from the premises of this Department without the explicit permission of the records manager in consultation with the Deputy Information Officer.

11.4. 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 Deputy Information Officer.

11.5. Personal information shall be managed in terms of the Protection of Personal Information Act 4 of 2013, as stipulated in paragraph 17 of this policy.

11.6. No staff member shall disclose personal information of any member of staff or client of the Department to any member of the public without consent by the officer first.

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

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

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

11.8.2. Access to registry and other storage areas is restricted to registry personnel unless stated otherwise.

12. Transfer of records

12.1. The Records Manager shall supervise the transfer of all records to an appropriate archives repository or another institution.

12.2. The Records Manager shall inform the Provincial Archivist in writing when the records are transferred to another government body with the transfer list attached.

12.3. The Records Manager shall ensure that no public records are transferred to off-site storage without prior approval from the Provincial Archivist.

12.4. The Records Manager shall ensure that no records are permanently or temporary transferred to any person or institution outside of government unless the Provincial Archivist has granted authority.

13. Legal admissibility and evidential weight

The Records Manager of the KZN Department of Human Settlements shall at all times contain reliable evidence of business operations, ensuring the adherence to the KZN Archives Act, 8 of 2011, Promotion of Access to Information Act , 2 of 2000, Protection of Personal Information Act 4 of 2013 and all other regulatory prescripts of the Department . The following shall then apply:

13.1. Paper-based records

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

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

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

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

13.2. Electronic records

13.2.1. 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, and
- in line with the National Archives and Records Service Act, 43 of 1996 and KZN Archives and Records Services Act 8 of 2011.

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

14.CLASSIFICATION OF FILES

Type of information	Category	Classification	Reason
1. Personnel	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual.
2. Information with regards to HIV status of employees	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual.
3. Home address and private contact details of employees	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual.

Type of information	Category	Classification	Reason
4. Salary scales and structures	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual.
5. Interviews summaries	Trade/departmental	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual. As a department secret, disclosures can cause disruption of ordered administration within the department.
6. Appointments	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual. As a department secret, disclosures can cause disruption of ordered administration within the department.
7. Financial records of the department	Trade/departmental	Confidential	Constitutes a trade secret, disclosure would cause financial loss or may cause embarrassment to the department in its relations with its clients, outside contractors, competitors and suppliers. As a state secret, disclosure would be harmful to the security or interests of the department.
8. Tender documents of the department	Trade	Secret	Constitute a trade secret, disclosure would cause financial loss or may cause embarrassment to the department in its relations with its clients, outside contractors and suppliers.
9. Applications	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual.
10. Declaration and disclosure of interest	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual.
11. Assets register	Departmental	Confidential	Constitute a departmental secret; disclosure can cause disruption of ordered administration within the department.
12. Investigation file	Personal/departmental	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause

Type of information	Category	Classification	Reason
			undue damage to the integrity and/ or reputation of individual.
13. Information with regards to the transport of cash handled by the department	Departmental	Secret	Constitutes a departmental secret, disclosure would be harmful to the security or interests of the department. It can also disrupt the effective functioning of the department.
14. Security audit reports	Departmental	Confidential	Constitutes a departmental secret, disclosure would be harmful to the security or interests of the department. It can also disrupt the effective functioning of the department.
15. Security plan	Departmental	Confidential	Constitutes a departmental secret, disclosure would be harmful to the security or interests of the department. It can also disrupt the effective functioning of the department.
16. Payroll reports	Trade	Confidential	Constitutes a trade secret, disclosure of would cause serious financial loss to the department. It can also disrupt it effective functioning.
17. Grievances	Personal	Confidential	Constitutes personal information, disclosure would cause a serious and irreparable encroachment on the privacy of an individual and may cause undue damage to the integrity and/ or reputation of individual.
18. Courier services	Trade	Confidential	Constitutes a trade secret, disclosure of would cause serious financial loss to the department. It can also disrupt it effective functioning.
19. Postage services	Trade	Confidential	Constitutes a trade secret, disclosure of would cause serious financial loss to the department. It can also disrupt it effective functioning.
20. MANCO and HEAC's meeting minutes	Departmental	Confidential	Constitutes a departmental secret, disclosure would be harmful to the security or interests of the department. It can also disrupt the effective functioning of the department.
21. Operational database with restricted access (BAS, Persal, Hardcat,etc)	Departmental	Confidential	Constitutes a departmental secret, disclosure would be harmful to the security or interests of the department. It can also disrupt the effective functioning of the department.

15. Training

15.1 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.

15.2 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.

15.3 The Records Manager shall ensure that all staff members are aware of the records management policies, in consultation with Unit Managers and shall conduct or arrange

such training as is necessary for the staff to equip them for their records management duties.

16. Inspection by the KZN Archives and Records Services

16.1. Section 18 (6) of the KZN Archives and Records Services Act 8 of 2011, stipulates that the KZN Archives Services is entitled to free and full access to all public records in the custody of all governmental bodies.

16.2. The Departmental Records Manager shall also conduct random records management inspections throughout the Department of Human Settlements including the Regional and District offices.

17. Processing of personal information held by the Department.

17.1. All personal information held by the Department of Human Settlements shall be processed in compliance with the conditions as set out in chapter 3 of the Protection of Personal Information Act, 04 of 2013 and in the Privacy Standards of the KZN Department of Human Settlements.

17.2. In terms of Condition 3: Purpose specification of POPIA:

17.2.1. The Department shall not retain personal information longer than is necessary for achieving the purpose for which it was collected or subsequently processed.

17.2.2. The Department shall only retain personal information longer if the retention of the record is required or authorized by law, the information owner has consented to the retention, retention of the record is required by a contract between parties thereto and if the department requires the record for lawful purposes related to departmental functions or activities.

17.2.3. The Department shall restrict processing of personal information if its accuracy is contested by the information owner, for a period enabling the responsible party to verify the accuracy of the information and if the department no longer need the personal information for achieving the purpose for which the information was collected but has to be maintained for the purpose of proof.

17.2.4. The Department shall restrict processing of personal information if the processing is unlawful and the information owner opposes its destruction or deletion and requests the restriction of its use or the information owner requests to transmit the personal information into another automated processing system.

17.3. Condition 7: Security safeguards of POPIA requires that:

17.3.1. The Department shall ensure that the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organizational measures to prevent loss of, damage to or unauthorized destruction of personal information and unlawful access to or processing of personal information.

17.3.2. In order to ensure safety, integrity and confidentiality of personal information the Department shall identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control, establish and maintain appropriate safeguards against the risks identified, regularly verify that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

17.3.3. The Department shall have due regard to generally accepted information security practices and procedures which may apply to it generally or required in terms of specific industry of professional rules and regulations.

17.3.4. **Information processed by service provider or person acting under authority**

17.3.4.1. A service provider or anyone processing personal information on behalf of a the KZN Department of Human Settlements must process such information only with the knowledge or authorization of the Department and treat personal information which comes to their knowledge as confidential and must not disclose it unless required by the law or in the course of the proper performance of their duties.

17.3.4.2. The Department shall, in terms of a written contract between the Department and a service provider, ensure that the service provider which processes personal information for the Department establishes and maintains effective security measures to prevent loss of, damage to or unauthorized destruction of personal information and unlawful access to or processing of personal information. The service provider shall notify the Department immediately where there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorized person.

18. **Manner of access**

18.1. A request for access to personal information must be made in the prescribed form to the information officer of the Department at his or her address or fax number or electronic mail address.

18.2. A request must be made in writing in compliance with the with sections 18 and 53 of the Promotion of Access to Information Act, 02 of 2000 and section 23 of the Protection of Personal Information Act , 04 of 2013.

18.3. Should the information owner have any complaint regarding private information held by the Department they must log a complaint with the Deputy Information Officer, who should handle the complaint in terms of the Promotion of Access to Information Act (PAIA) Manual.

19. Ownership of records

19.1. All records, irrespective of format, (i.e. paper and electronic, including e-mails and other records) created or received by employees in the course of their duties, are the property of the KZN Department of Human Settlements and subject to its overall control.

19.2. Employees leaving the KZN Department of Human Settlements or changing positions within the Department are required to leave all records for their successors.

20. Monitoring and review

20.1. The Records Manager should ensure the establishment of a registry in all regions with trained designated registry officials.

20.2. The records manager shall review the record keeping and records management practices of the KZN Department of Human Settlements on a regular basis and shall adapt them appropriately to ensure that it is being maintained without deficiencies, irregularities, and misunderstanding.

20.3. It should be adapted appropriately to ensure that it meets the business and service delivery requirements of the Department. The policy should be amended as and when it is required.

20.4. This policy should be reviewed in terms of the following criteria:

- Flexibility
- Reliability
- Simplicity
- Usability
- Cost-effective
- Consistency
- Responsiveness to user needs
- And other Archives Regulations

21. References

- Approved Records Management Policy for the KZN Department of Public Works,
- Approved Records Management Policy for Kwazulu Natal Treasury
- EThekwini Municipality's Records Management Policy
- National Archives Records Management Policy Prototype.

22. Approval

Approved

MR. MOS ZUNGU
HEAD OF DEPARTMENT

7/03/2013

DATE